United States Government Accountability Office

Report to Congressional Requesters

December 2021

VIRTUAL CURRENCIES

Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking

Accessible Version

GAO@100
A Century of Non-Partisan Fact-Based Work

GAO-22-105462

GAO Highlight

Highlights of GAO-22-105462, a report to congressional requesters

December 2021

VIRTUAL CURRENCIES

Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking

Why GAO Did This Study

Virtual currencies are an emerging payment method for transactions, such as retail purchases. Virtual currency's anonymizing features can attract criminals' use to avoid detection when paying for illicit activities, such as human and drug trafficking. Thus, policy makers, regulators, and law enforcement have identified virtual currency, human trafficking, and drug trafficking as priority areas of concern.

GAO was asked to review the use of virtual currency to facilitate sex and drug trafficking. This report examines (1) the use of virtual currency for human and drug trafficking and the extent to which U.S. agencies collect data on these topics; and (2) the extent to which U.S. agencies have taken steps to counter human and drug trafficking facilitated by virtual currency and challenges these agencies face. GAO analyzed data, reviewed documentation, and interviewed relevant officials at selected federal agencies.

What GAO Recommends

GAO made 2 recommendations in this public report, including that FinCEN and IRS review virtual currency kiosk registration requirements. FinCEN and IRS concurred.

View GAO-22-105462. For more information, contact Gretta L. Goodwin at (202) 512-8777 or goodwing@gao.gov or John Pendleton at (202) 512-3489 or pendletonj@gao.gov.

What GAO Found

This is a public version of a sensitive report that GAO issued in September 2021. Therefore, this report omits sensitive information and data on selected federal agencies' activities to counter human and drug trafficking, associated use of virtual currency, and related challenges.

Virtual currency is increasingly used illicitly to facilitate human and drug trafficking, according to GAO's review of agency documentation and data and interviews with officials. For example, the number of suspicious activity reports filed with the Financial Crimes Enforcement Network (FinCEN) that involve virtual currency and drug trafficking increased fivefold (from 252 to almost 1,432) from calendar year 2017 to 2020. However, in a sensitive version of this report, GAO found that data from selected federal agencies on virtual currency use for human and drug trafficking may not be consistently captured. Consequently, agencies may lack complete data when assessing or reporting on the illicit use of virtual currency in human and drug trafficking. In that report GAO made nine recommendations to selected agencies to enhance their data collection practices.

Example of Virtual Currency Kiosk, Which May Be Used in Human and Drug Trafficking

Source: U.S. Immigration and Customs Enforcement. | GAO-22-105462

Selected federal agencies have taken actions to counter the illicit use of virtual currency in human and drug trafficking but face challenges. For example, FinCEN and the Internal Revenue Service (IRS) oversee virtual currency entities. FinCEN imposes requirements for operators of virtual currency kiosks that are used to exchange virtual currencies for cash and are found in various locations such as convenience stores (see fig.). While kiosk operators are required to register with FinCEN, they are not required to routinely report the specific locations of their kiosks. This limits federal agencies' ability to identify kiosks in areas that have been designated as high risk for financial crimes and could involve human and drug trafficking. Reviewing registration reporting requirements and taking appropriate action, as needed, to better identify individual kiosk locations by operator could help FinCEN and IRS identify high-risk kiosk operators to monitor for compliance, while also improving information law enforcement has available to identify potentially illicit transactions.

Contents

Tables

Figures

Abbreviations

AML Act	Anti-Money Laundering Act of 2020
BSA/AML	Bank Secrecy Act / anti-money laundering
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DOJ	Department of Justice
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FinCEN	Financial Crimes Enforcement Network
ICE-HSI	Immigration and Customs Enforcement - Homeland Security Investigations
IRS	Internal Revenue Service
IRS-CI	IRS Criminal Investigation
JCODE	Joint Criminal Opioid Darknet Enforcement
MSB	money services business
OFAC	Office of Foreign Assets Control
TFI	Office of Terrorism and Financial Intelligence
SAR	Suspicious Activity Report
USPS	U.S. Postal Service

441 G St. N.W.
Washington, DC 20548

December 8, 2021

The Honorable Andy Barr
Ranking Member
Subcommittee on National Security,
International Development, and Monetary Policy
Committee on Financial Services
House of Representatives

The Honorable J. French Hill
House of Representatives

Virtual currencies—digital representations of value, usually other than government-issued legal tender—are an emerging payment method.[1] As of September 2021, the total market capitalization of all virtual currencies was about $2.2 trillion, according to one index.[2] Virtual currencies are increasingly being used as a payment method in various transactions, such as making purchases at retailers. However, virtual currencies can also facilitate illicit activities, including human and drug trafficking.[3] A July 2020 report by Polaris, a nonprofit organization knowledgeable about human trafficking, found that virtual currency was the second-most commonly accepted payment method on 40 platforms in the online commercial sex market—which has been used to facilitate sex

[1]For the purposes of this report, we use the term "virtual currency" to include convertible virtual currencies, such as cryptocurrencies, and other industry labels such as digital assets and virtual assets.

[2]Total market capitalization is the sum of individual virtual currencies' market capitalizations, which CoinMarketCap determines by calculating the average price of a virtual currency multiplied by the circulating supply of that virtual currency, https://coinmarketcap.com/charts, accessed September 1, 2021.

[3]Human trafficking generally refers to the exploitation of adults by force, fraud, or coercion, or of a child under the age of 18 by any means, for such purposes as forced labor, involuntary servitude or commercial sex. See 22 U.S.C. § 7102(3) (coercion), (4) (commercial sex act), (8) (involuntary servitude), (11) (severe forms of trafficking in persons), (12) (sex trafficking). The primary human trafficking criminal statutes are at 18 U.S.C. chs. 77 (§§ 1581-1597), 117 (§§ 2421-2429); see in particular 18 U.S.C. §§ 1584 (involuntary servitude), 1589 (forced labor), 1591 (sex trafficking). Drug trafficking generally refers to the illicit production, transportation, and distribution of controlled substances by an individual or drug trafficking organization in violation of U.S. criminal law.

trafficking.[4] Moreover, we recently reported that platforms in the online commercial sex market accept virtual currency.[5] Additionally, according to the Department of Justice (DOJ), virtual currency is increasingly used to buy and sell illegal drugs on Dark Web marketplaces and by drug cartels to launder their profits, contributing to a drug epidemic, which the Centers for Disease Control and Prevention reported killed over 70,600 Americans by overdose in 2019 alone.[6]

The Bank Secrecy Act and its implementing regulations generally require financial institutions to collect and retain various records of customer transactions, verify customers' identities, maintain anti-money laundering (AML) programs, and report suspicious transactions—including suspected human and drug trafficking.[7] Although the existing regulatory framework includes methods to counter illicit activity involving virtual currency, virtual currencies are relatively new and have the potential to create vulnerabilities within the financial system that pose regulatory and enforcement challenges. For instance, some virtual currencies allow for a degree of anonymity in domestic and cross-border payments, which can make it difficult for financial institutions and law enforcement to identify and trace illicit transactions.[8] The illicit use of virtual currency, human trafficking, and drug trafficking are priority areas of concern for regulators, law enforcement, and national security. Therefore, all three were included

[4]Polaris, *Using an Anti-Money Laundering Framework to Address Sex Trafficking Facilitated by Commercial Sex Advertisement Websites* (July 2020).

[5]GAO, *Sex Trafficking: Online Platforms and Federal Prosecutions*, GAO-21-385 (Washington, D.C.: June 2021). We refer to the online commercial sex market as the online promotion of in-person commercial sex acts, whether through prostitution, which is illegal in all states but Nevada; or sex trafficking, which is a federal crime and with respect to which all 50 states and the District of Columbia have criminal statutes that can be used for antitrafficking efforts.

[6]Department of Justice, Office of the Deputy Attorney General, Cyber Digital Task Force, *Cryptocurrency Enforcement Framework* (Washington, D.C.: October 2020).

[7]Currency and Foreign Transactions Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified, as amended, primarily at 31 U.S.C. §§ 5311, *et seq.*, among other places in the U.S. Code) (commonly referred to as the "Bank Secrecy Act").The Bank Secrecy Act imposes a range of recordkeeping and reporting obligations across a wide sector of financial institutions, compliance with which is essential to detecting, investigating, and deterring criminal activity, according to DOJ officials. There are civil and criminal penalties for willful Bank Secrecy Act violations, including failure to report suspicious activity, such as suspected human and drug trafficking.

[8]GAO, *Virtual currencies: Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges*, GAO-14-496 (Washington, D.C.: May 29, 2014).

in the first government-wide priorities for anti-money laundering and countering the financing of terrorism policy, which were issued in June 2021.[9]

Various agency components within the Department of the Treasury (Treasury), the Department of Homeland Security (DHS), and DOJ are responsible for enforcing U.S. laws and regulations related to the use of virtual currencies. You asked us to review the flow of money from virtual currencies and online marketplaces to buy, sell, or facilitate the financing of goods or services associated with sex trafficking and drug trafficking. We examined (1) what is known about the use of virtual currency for human and drug trafficking and the extent to which U.S. agencies collect data on these topics; and (2) the extent to which U.S. agencies have taken steps to counter human and drug trafficking facilitated by the use of virtual currency, and the challenges, if any, these agencies face.

This is a public version of a sensitive report that we issued in September 2021. DOJ deemed some of the information in our September report as sensitive, which must be protected from public disclosure. Therefore, this report omits sensitive information on selected federal agencies' data collection methods and activities to counter human and drug trafficking facilitated by the use of virtual currency, and what challenges, if any, these agencies face.[10] Although the information provided in this report is

[9]The Anti-Money Laundering Act of 2020 requires the Secretary of the Treasury, in consultation with the Attorney General, federal functional regulators, relevant state financial regulators, and relevant national security agencies, to establish and make public, within 180 days of enactment, priorities for anti-money laundering and countering the financing of terrorism policy. Pub. L. No. 116-283, div. F, title LXI, § 6101(b)(2)(C), 134 Stat. 3388, 4550-51 (2021). Accordingly, the U.S. Department of the Treasury's Financial Crimes Enforcement Network published the first national Anti-Money Laundering/Countering the Financing of Terrorism National Priorities on June 30, 2021. See Financial Crimes Enforcement Network, *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities* (June 30, 2021). FinCEN identified cybercrime, including virtual currency considerations; human trafficking; and drug trafficking organization activity, as three of the eight national priorities announced in June 2021.

[10]The agencies included Immigration and Customs Enforcement's Homeland Security Investigations (ICE-HSI), the Secret Service, Drug Enforcement Administration (DEA), Federal Bureau of Investigation (FBI), DOJ's Criminal Division, DOJ's Justice Management Division, IRS Criminal Investigations, FinCEN, and Postal Inspection Service.

more limited, the report addresses the same objectives as the sensitive report and uses the same methodology.[11]

To inform both objectives, we purposively selected and interviewed officials from 14 federal components that had the most extensive or specific expertise with virtual currency as it relates to human and drug trafficking.[12] We identified these components by interviewing officials at DOJ, DHS, Treasury, the U.S. Postal Service (USPS), the Office of National Drug Control Policy, the Department of State, and the Department of Labor and reviewing information provided by these agencies' components (e.g., subagencies, divisions, units). We also selected and interviewed a nongeneralizable sample of representatives from five third-party organizations actively involved in analyzing virtual currency or combatting human trafficking.[13] We identified these third parties by asking agency officials and reviewing our prior work. Information collected through the interviews cannot be generalized to all U.S. components or third parties but provides useful information to address both of our objectives. Further, to inform both objectives, we reviewed agency documentation and applicable federal laws, regulations, and guidance.

To examine the extent to which U.S. agencies have taken steps to counter human and drug trafficking facilitated by the use of virtual currency, and what challenges, if any, these agencies face, we reviewed guidance, proposed rules, and documentary evidence of U.S. agencies' efforts to counter human and drug trafficking that involve virtual

[11]GAO, *Virtual Currencies: Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking*, GAO-21-104129SU (Washington, D.C.: Sept 30, 2021).

[12]Throughout this report, we refer to components of federal agencies (e.g., subagencies, divisions, units). When we refer to the department level (e.g., DOJ, DHS, Treasury, USPS), we use the term "agencies." We also met with additional federal components such as the Secret Service and the Internal Revenue Service's (IRS) Small Business/Self Employed Division to further inform our assessment of federal efforts regarding the use of virtual currency in human and drug trafficking.

[13]We selected two blockchain analytics firms that focus on virtual currency and three nonprofits focused on combatting human trafficking. The two blockchain analytics firms interviewed included Chainalysis and CipherTrace. The three human trafficking nonprofit organizations we identified included the Human Trafficking Institute, the Human Trafficking Legal Center, and Polaris. The Human Trafficking Institute and the Human Trafficking Legal Center conduct human trafficking research. Polaris works to prevent and reduce sex and labor trafficking in the United States and Mexico and, since 2007, has operated the National Human Trafficking Hotline.

currency.[14] To examine Treasury's efforts to oversee virtual currency entities, we interviewed officials from FinCEN's Enforcement and Compliance Division and the Internal Revenue Service's (IRS) Small Business/Self-Employed Division and reviewed registration requirements, examination practices, and enforcement actions.[15]

To examine Treasury's efforts to oversee virtual currency kiosks—stand-alone machines that facilitate the buying, selling, and exchange of virtual currencies—we reviewed FinCEN data on registered and unregistered operators of virtual currency kiosks. We assessed these data by discussing it with agency officials and comparing data on kiosk operators with a public website described below. We found these data to be sufficiently reliable for the purposes of providing the number of registered kiosks and FinCEN's estimates for the number of unregistered kiosks that it has identified.[16] We reviewed a public website that provides data on virtual currency kiosks and the number of kiosks under the top operators, operating the largest number of kiosks.[17] We assessed the reliability of information posted on this website by discussing it with agency officials and comparing the information on the top 10 kiosk operators identified on the website with information available to law enforcement. We found information posted on this website to be sufficiently reliable for estimating the number of kiosks for large operators.[18] We compared Treasury's oversight of virtual currency kiosks with criteria in the AML Act and

[14]Generally, documentary evidence was from the 14 selected federal components, and from additional components with which we held separate targeted interviews, such as the Secret Service and IRS's Small Business/Self-Employed Division.

[15]For registration requirements, we reviewed money services businesses regulations and filing instructions described in Financial Crimes Enforcement Network, *Registration of Money Services Business (RMSB) Electronic Filing Instructions,* version 1.0 (July 2014).

[16]FinCEN officials identified kiosks by researching open source information, such as articles and social media, and publicly available money services business registration data to identify registered and unregistered virtual currency kiosk. FinCEN officials stated that due to the nature of identifying unregistered entities, there are inherent limitations in knowing the full number of kiosk providers operating in the United States.

[17]https://coinatmradar.com/charts/top-operators/.

[18]Further, since the website allows operators of virtual currency kiosks to self-report kiosk locations so that users can locate virtual currency kiosks and utilize their services there is financial incentive for kiosk operators to accurately report and update the website.

international anti-money laundering standards.[19] For more information on our scope and methodology, see appendix I.

We conducted this performance audit from February 2020 to September 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We subsequently worked with DOJ, from October 2021 to December 2021 to prepare this version of the original sensitive report for public release. This public version was also prepared in accordance with these standards.

Background

Human Trafficking

Human trafficking is the exploitation of a person, typically through force, fraud, or coercion, for such purposes as forced labor, involuntary servitude, or commercial sex.[20] Human trafficking often involves victims

[19]See Financial Action Task Force, *International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation, FATF Recommendations* (Paris, France: October 2020); and Pub. L. No. 116-283, div. F, title LXII, § 6216, 134 Stat. at 4582-83.

[20]Federal law generally recognizes two forms of human trafficking—sex trafficking and labor trafficking. The Trafficking Victims Protection Act of 2000, as amended, defines sex and labor trafficking under the term "severe forms of trafficking in persons," the substance of which is largely mirrored by the act's related criminal provisions. These severe forms of trafficking are (1) sex trafficking in which a commercial sex act is induced by force, fraud, or coercion, or in which the person induced to perform such act has not attained 18 years of age; or (2) the recruitment, harboring, transportation, provision, or obtaining of a person for labor or services, through the use of force, fraud, or coercion, for the purpose of subjection to involuntary servitude, peonage, debt bondage, or slavery. See Pub. L. No. 106-386, div. A, §§ 103, 112(a)(2), 114 Stat. 1464, 1469-71, 1486-90 (classified, as amended, at 22 U.S.C. § 7102(3) (coercion), (4) (commercial sex act), (8) (involuntary servitude), (11) (severe forms of trafficking in persons), (12) (sex trafficking); and criminal provisions codified, as amended, at 18 U.S.C. §§ 1584 (involuntary servitude), 1589 (forced labor), 1591 (sex trafficking)). For the primary human trafficking criminal statutes, see 18 U.S.C. chs. 77 (§§ 1581-1597), 117 (§§ 2421-2429). Human trafficking is a crime that is a predicate offense to money laundering. Human trafficking is separate from human smuggling, which need not involve exploitation and is the act of bringing into, or harboring/transporting within the United States, certain foreign individuals who are not permitted to lawfully enter or remain in the United States. See 8 U.S.C. §§ 1323-24.

who are already vulnerable—such as missing and runaway youth or persons dealing with substance abuse addictions—but can include victims from varied backgrounds, such as race, ethnicity or sexuality.[21]

There is no reliable estimate of the number of trafficking victims in the United States or of the money generated by this crime.[22] According to the Department of State, the quality and quantity of data available are often hampered by the hidden nature of the crime, challenges in identifying individual victims, gaps in data accuracy and completeness, and significant barriers regarding the sharing of victim information. While the number of victims may not be fully reflected, prosecutorial and investigative efforts to combat human trafficking provide some insight on the scope and breadth of trafficking victims. For example, during fiscal year 2019, DOJ and DHS collectively opened 1,631 investigations related to human trafficking, according to Department of State's annual report on global efforts to eliminate trafficking.[23] At the same time, DOJ initiated a total of 220 federal human trafficking prosecutions and secured convictions against 475 traffickers.[24]

Drug Trafficking

Drug trafficking is the illicit production, transportation, and/or distribution of controlled substances by an individual or drug trafficking organization in violation of U.S. criminal law.[25] Nationally, rates of drug misuse have increased in recent years. According to the Substance Abuse and Mental Health Services Administration, an estimated 20.8 percent of the U.S. population (57.2 million people) used illicit drugs in 2019, an increase

[21]GAO, *Human Trafficking: Agencies Have Taken Steps to Assess Prevalence, Address Victim issues, and Avoid Grant Duplication*, GAO-16-555 (Washington, D.C.: June 28, 2016)

[22]The Department of State does not internally track human trafficking cases that may have involved virtual currency, therefore, it is unclear the extent to which virtual currency is involved, according to department officials.

[23]U.S. Department of State, *Trafficking in Persons* Report, 20th ed. (Washington, D.C.: June 2020). DOJ opened a total of 607 investigations, while DHS opened 1,024 investigations.

[24]U.S. Department of State, *Trafficking in Persons* Report, 20th edition.

[25]In particular, *see* 21 U.S.C. § 841. *See generally* 21 U.S.C. §§ 841-65 (offenses and penalties), §§ 951-71 (import and export), 46 U.S.C. ch. 705 (maritime drug law enforcement).

from an estimated 17.8 percent (or 47.7 million people) in 2015, the earliest year for which data are available.[26] Nationally representative data show that this increase in the estimated rate of drug misuse has occurred across several demographic categories, such as sex and education levels.[27]

Virtual Currency

Virtual currencies are digital representations of value that are usually not government-issued legal tender. While there is no generally applicable statutory definition for virtual currency, under the AML Act (January 2021), it is referred to as an emerging payment method that functions as a form of value substituting for currency, funds, or other monetary instruments.[28] Additionally, in its 2013 guidance, FinCEN defines "virtual" currency as a medium of exchange that operates like a currency in some

[26]Substance Abuse and Mental Health Services Administration, *Key Substance Use and Mental Health Indicators in the United States: Results from the 2019 National Survey on Drug Use and Health,* HHS Publication No. PEP20-07-01-001, NSDUH Series H-55 (Rockville MD: 2020). The National Survey on Drug Use and Health considers that illicit drugs include marijuana, pain reliever misuse, hallucinogens, tranquilizer or sedative misuse, cocaine, stimulant misuse, inhalants, and heroin. Due to methodological changes, years prior to 2015 are not comparable or available.

[27]GAO, *Drug Misuse: Sustained National Efforts Are Necessary for Prevention, Response, and Recovery*, GAO-20-474 (Washington, D.C.: March 2020).

[28]The AML Act was enacted as Division F of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, div. F, title LXI, § 6102(a)(3), (d), 134 Stat. 3388, 4552-53 (codified at 31 U.S.C. §§ 5312(a)(1)-(3), 5330(d)). ("[A]lthough the use and trading of virtual currencies are legal practices, [illicit actors]… increasingly rely on substitutes for currency, including emerging payment methods (such as virtual currencies)."), (d), 134 Stat. 3388, 4552-53 (codified at 31 U.S.C. §§ 5312(a)(1) ("financial agency" is a person acting for a person as a financial institution or in another role, related to various forms of value, including "value that substitutes for currency"), (2) ("financial institution" includes certain entities transmitting (or exchanging) value that substitutes for currency (or funds)), (3) (By regulation, "monetary instruments" may include "value that substitutes for any monetary instrument described in subparagraph (A), (B), or (C)"), 5330(d)(1) ("money transmitting business" includes, among others, a person who engages as a business in transmission of currency, funds, or value that substitutes for currency.), (2) ("money transmitting service" includes accepting currency, funds or value that substitutes for currency and transmitting the currency, funds or value that substitutes for currency by any means). As further background, FinCEN's December 2020 Notice of Proposed Rulemaking proposes, among other things, to prescribe by regulation that convertible virtual currency and digital assets with legal tender status are monetary instruments for purposes of the BSA. Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 85 Fed. Reg. 83,840 (Dec. 23, 2020) (to be codified at 31 C.F.R. pts. 1010, 1020, 1022).

environments but does not have all the attributes of real currency—such as legal tender status.[29]

Virtual Currency Wallets

Virtual wallets are software programs that allow people to "store" their virtual currency.

Virtual wallets do not store virtual currency like traditional wallets store cash. Instead, they store various components of virtual currency transactions, such as private keys, public keys, and addresses that allow the user to gain access to the currency. Virtual wallets come in various forms, including web-based, desktop, mobile, paper, and hardware—such as a USB stick.

- Private keys are a series of alphanumeric characters that work similarly to a personal identification number (PIN) or password that prove ownership of the virtual currency. Private keys are used to sign virtual currency transactions. Each virtual wallet can have multiple private keys.
- Public keys are a series of alphanumeric characters generated from a virtual wallet's private key that create addresses that can receive virtual currency. A wallet can create an unlimited number of addresses.

Source: GAO and GAO analysis of federal entities documentation. | GAO-22-105462

Unlike U.S. dollars and other government-issued currencies, virtual currencies do not necessarily have a physical coin or bill associated with their circulation. Some virtual currencies may be used to purchase goods and services in the real economy and can be converted into government-issued currencies through virtual currency exchanges. For example, some retailers, including Microsoft, Overstock, AT&T, and Home Depot, accept virtual currency as a form of payment. Virtual currency transactions can occur online through a network that can be accessed using wallet software (see sidebar). Other virtual currencies can only be used within virtual economies (e.g., within online role-playing games) and may not be readily exchanged for government-issued currencies such as U.S. dollars, European Union euro, or Japanese yen.[30]

Companies and individuals that offer virtual currency and other virtual asset exchange services are often referred to as "exchanges" and "exchangers." For example, there are traditional virtual currency exchanges that are online trading platforms that facilitate virtual currency transactions between buyers and sellers. Individual exchangers, typically individuals who buy and sell virtual currency, are also known as peer-to-peer exchangers.[31] Virtual currency can also be exchanged for fiat cash (government-issued legal tender such as the U.S. dollar) or other virtual currencies by virtual currency kiosks (kiosks). Similarly, virtual currency

[29]Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001 (Mar. 18, 2013). In 2019, FinCEN clarified that convertible virtual currency is a type of virtual currency that either has an equivalent value as currency, or acts as a substitute for currency, and is therefore a type of "value that substitutes for currency." Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001 (May 9, 2019).

[30]Virtual currencies used within virtual economies, such as online role-playing games, were outside the scope of this review.

[31]Further, there are decentralized exchanges that can be used to swap virtual currency for other types of virtual currency. These decentralized exchanges are software programs that operate on a peer-to-peer network of computers running a blockchain platform designed such that they may not be controlled by a single person or group of persons (that is, they do not have an identifiable administrator).

kiosks can also sometimes exchange fiat cash for virtual currency (see sidebar).[32]

Virtual Currency Kiosks

Virtual currency kiosks (kiosks) are stand-alone machines that facilitate the buying, selling, and exchange of virtual currencies.

Kiosks can be found in various locations, such as malls, convenience stores, gas stations, and grocery stores.

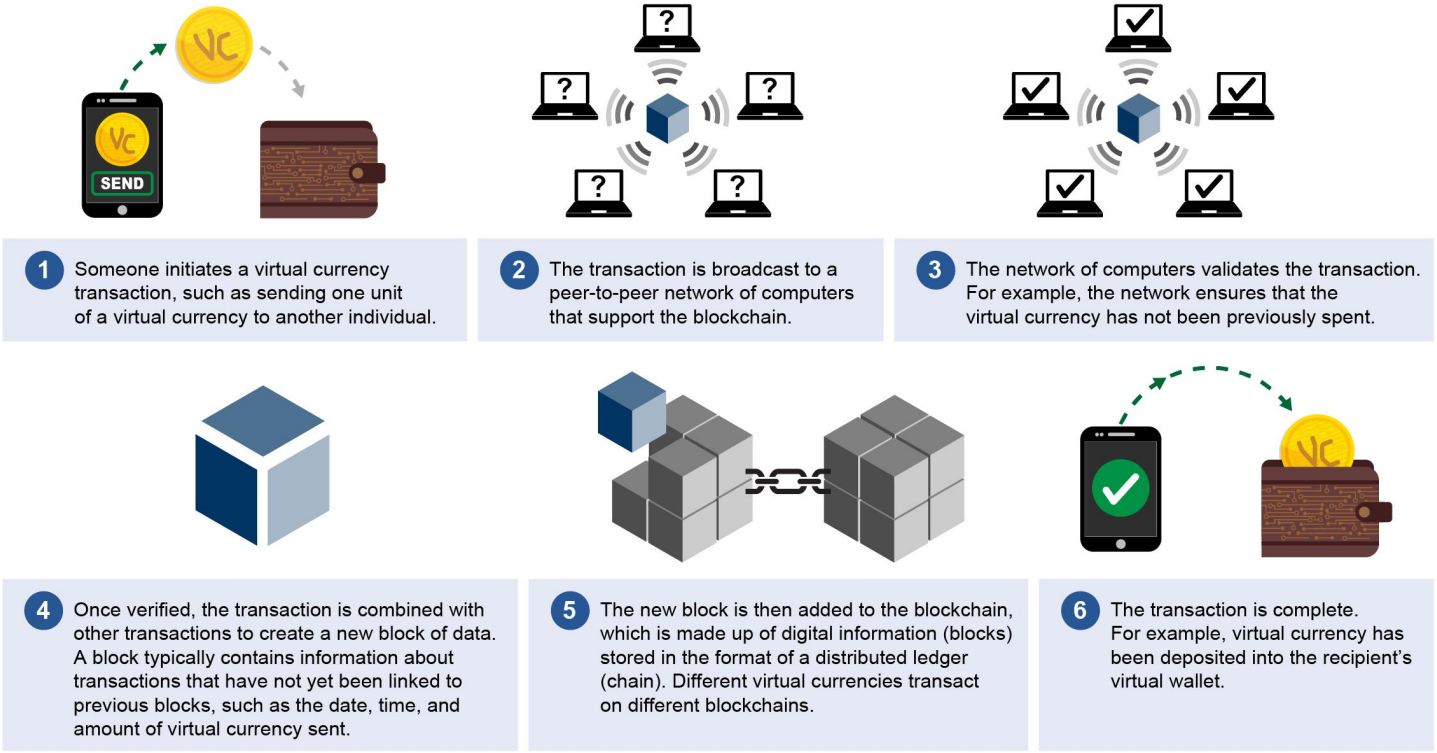
Source: GAO analysis of DOJ documents including the Attorney General's Cyber Digital Task Force, *Cryptocurrency Enforcement Framework*., U.S. Immigration and Customs Enforcement (photo). | GAO-22-105462

Many virtual currencies in use today record transactions on a blockchain (see fig. 1). A blockchain is a type of distributed ledger technology that is made up of digital information (blocks) recorded in a public or private database in the format of a distributed ledger (chain).[33] The ledger permanently records the history of transactions that take place among the participants within the network in a chain of cryptographically secured blocks. Depending on the technical specifications of a virtual currencies' blockchain, each virtual currency transaction can generate new and unique addresses. Cryptocurrency is a type of virtual currency that employs encryption technology and usually operates on a blockchain. Bitcoin, which emerged in 2009, is the first and most widely circulated blockchain-based cryptocurrency.

[32]Kiosks are rapidly increasing in the U.S., growing from about 560 in January 2017 to over 22,600 as of September 1, 2021, according to information from kiosk crowdsourcing website coinatmradar.com. This website allows operators of virtual currency kiosks to self-report kiosk locations so that users can locate virtual currency kiosks and utilize their services. See https://coinatmradar.com/charts/growth/united-states/ accessed September 1, 2021.

[33]Distributed ledger technology allows for users across a computer network to verify the validity of transactions potentially without a central authority.

Figure 1: Example of How Virtual Currency Can Operate Using Blockchain, a Distributed Ledger Technology



Source: GAO. | GAO-22-105462

Virtual currency's global nature, potential anonymizing features, increasing accessibility, and ease of use in online marketplaces can attract criminals' use to avoid detection while facilitating various illicit activities, including laundering proceeds from human and drug trafficking.[34] Although collecting certain information is generally required, some virtual currency entities such as peer-to-peer exchanges and virtual currency kiosks may choose not to collect information about a user's identity, providing some degree of anonymity and making virtual currencies attractive to criminals. Further, criminals can also use anonymity-enhanced virtual currencies and methods, such as "mixers" or "tumblers," in an attempt to conceal illicit transactions used to facilitate criminal activities. See appendix II for additional information on these

[34]Bitcoin is the most commonly used virtual currency that agencies have observed facilitating illicit activities, according to officials from several federal agencies we interviewed.

methods. Officials from several federal components also told us that while virtual currencies may be used to facilitate illicit transactions on the Surface Web, Dark Web marketplaces are common venues in which these components have observed the use of virtual currency for facilitating criminal activities such as illicit drug trafficking.[35]

According to officials from several federal agencies, virtual currency can be used in a variety of crimes other than human and drug trafficking, such as the sale and purchase of other illicit goods and services on Dark Web marketplaces (e.g., firearms, forged identification documents, malware, computer hacking services, and child exploitative material). Officials also stated that virtual currency can be used in crimes such as selling personally identifiable information, money laundering, cryptocurrency fraud and Ponzi schemes, ransomware payments, and financing terrorist organizations.[36]

The Size of the Virtual Currency Market

The size of the virtual currency market is unknown due to limitations in available data, but there are data that may provide some context.[37]

- According to one index, the total market capitalization of virtual currency of any type was about $2.2 trillion as of September 2021

[35]For more information about anonymity-enhanced methods and online venues (i.e., Surface Web and Dark Web marketplaces) criminals have used to obfuscate and facilitate crimes with virtual currency, including human and drug trafficking, see app. II.

[36]According to officials from DOJ's Criminal Division, the Federal Bureau of Investigation (FBI), FinCEN, and the Secret Service, criminals frequently use virtual currency to facilitate fraud schemes and ransomware payments (a type of malware that prevents an individual from accessing computer files, systems, or networks and demands ransom pay). Ransomware is a particularly acute concern, as cybercriminals are using sophisticated attacks to target various sectors, including government, finance, education, and healthcare, according to FinCEN officials. FinCEN officials also stated that in most cases, ransomware operators use virtual currencies to receive payments from victims because the transactions can often be done without the involvement of a compliant financial institution.

[37]Given these limitations, we did not assess the reliability of these data. We provide some figures to provide context for the possible size of the virtual currency market.

compared with about $250 billion 2 years ago (September 2019).[38] The total market capitalization of Bitcoin, one of the most prominent virtual currencies, is estimated to be over $914 billion as of September 2021.[39] The fair market value of Bitcoin has changed dramatically over time. For example, the opening value of Bitcoin increased from about $960 in January 2017 to over $63,500 by April 2021 and as of September 1, 2021, had declined to just over $47,000.[40]

- As of September 1, 2021, 10 major virtual currency exchanges had collectively handled an average daily trading volume in Bitcoin of more than $4 billion, according to Bitwise, a virtual currency asset management company. For comparison, the Federal Reserve Banks' Automated Clearing House (a traditional payment processor) processed $1.8 billion in payment transactions on average per day in 2020.
- As of September 2021, Coinbase, a large U.S.-based virtual currency exchange, reported a user base of more than 68 million.

Financial Regulations and Several Federal Agencies Support Countering the Use of Virtual Currency in Human and Drug Trafficking

Bank Secrecy Act Framework

The Bank Secrecy Act and related anti-money laundering authorities and requirements (collectively, BSA/AML) are important tools used by regulators and law enforcement agencies to detect and deter the use of financial institutions for criminal activity, such as human and drug

[38]Total market capitalization is the sum of individual virtual currencies' market capitalizations, which CoinMarketCap determines by calculating the average price of a virtual currency multiplied by the circulating supply of that virtual currency. https://coinmarketcap.com/charts/, accessed September 1, 2021.

[39]https://www.blockchain.com/charts/market-cap, accessed September 2, 2021.

[40]The open value is the starting value of one bitcoin recorded each day, https://coinmarketcap.com/currencies/bitcoin/historical-data/, accessed September 13, 2021.

trafficking, including in cases where virtual currency is involved.[41] FinCEN serves as the financial intelligence unit of the United States and oversees the administration of the BSA and related AML regulations. The application of BSA/AML requirements depends on whether the entity operates as a covered type of financial institution. For example, much of the virtual currency activity in the United States is undertaken through intermediary financial institutions that meet FinCEN's definition of money transmitter. Therefore, FinCEN subjects those intermediaries to regulatory requirements applicable to money services businesses (MSB), of which money transmitters are one type.[42] For purposes of this report, we will focus on virtual currency activities engaged in by MSBs.

DOJ can conduct investigations and prosecute financial institutions and individuals for both civil and criminal violations of BSA/AML laws and regulations. In addition, several law enforcement agencies (discussed below) can conduct BSA-related criminal investigations.

Federal Agencies

A number of U.S. government agencies are involved in countering the illicit use of virtual currency for human and drug trafficking, shown in figure 2. Broadly, these agencies are characterized as either federal financial regulatory or law enforcement agencies, which include investigative and prosecutorial agencies.

- **Regulatory compliance and enforcement:** FinCEN has authority to enforce BSA/AML requirements, including through civil money

[41]BSA and its implementing regulations generally require financial institutions—such as banks, securities broker-dealers, futures and commodities brokers, and money transmitters—to collect and retain various records of customer transactions, verify customers' identities, maintain AML programs, and report suspicious transactions.

[42]Other requirements may apply if the entity operates as another type of financial institution, such as a bank or broker-dealer. FinCEN regulations define a money transmitter as a person that provides money transmission services, which means the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another person or location by any means. The definition of money transmitter also includes any other person engaged in the transfer of funds. 31 C.F.R. § 1010.100(ff)(5). Under FinCEN's BSA/AML regulations, money transmitters are a type of money services business (MSB). Other types of MSBs include, subject to exception, dealers in foreign exchange, check cashers, issuers or sellers of traveler's checks or money orders, providers or sellers of prepaid access (such as prepaid cards), and the U.S. Postal Service. *See* 31 C.F.R. § 1010.100(ff).

penalties. FinCEN is a bureau within Treasury that reports to Treasury's Under Secretary for Terrorism and Financial Intelligence (TFI). TFI includes other components actively involved in AML efforts.[43] FinCEN delegated authority to IRS's Civil Division to conduct BSA/AML examinations of MSBs, including virtual currency MSBs.[44] IRS's Civil Division does not have authority to impose penalties, but issues letters of noncompliance to institutions it oversees and generally relies on FinCEN for formal civil enforcement action.[45]

- **Investigative:** Investigative agencies within DOJ include the Drug Enforcement Administration (DEA) and the Federal Bureau of Investigation (FBI). Within DHS, the Immigration and Customs Enforcement's Homeland Security Investigations (ICE-HSI) and the U.S. Secret Service (Secret Service) also conduct criminal investigations, such as into the illegal cross-border movement of people, goods, and other contraband throughout the United States. The Secret Service investigates financial crimes, which include the illicit use of virtual currency and, at times, for human and drug trafficking. The USPS's U.S. Postal Inspection Service identifies and seizes trafficked drugs that come through the postal service. IRS's Criminal Investigation (IRS-CI) division conducts criminal investigations including those involving virtual currencies related to tax crimes, money laundering, and currency violations.
- **Prosecutorial:** Within DOJ, litigating divisions, such as the Criminal Division and U.S. Attorney's offices, enforce and prosecute violations of certain federal criminal laws involving virtual currencies, in

[43]In addition to FinCEN, Office of Terrorism and Financial Intelligence components include: (1) the Office of Foreign Assets Control, which administers and enforces sanctions based on national security and foreign policy priorities (2) the Office of Intelligence and Analysis, one of the 16 U.S. Intelligence Community members; (3) the Office of Terrorist Financing and Financial Crimes, which is responsible for formulating and coordinating anti-money laundering and countering the financing of terrorism policies and is also charged with developing and promoting AML and counter-terrorist financing international standards; and (4) the Treasury's Executive Office for Asset Forfeiture, which administers the Treasury's Forfeiture Fund.

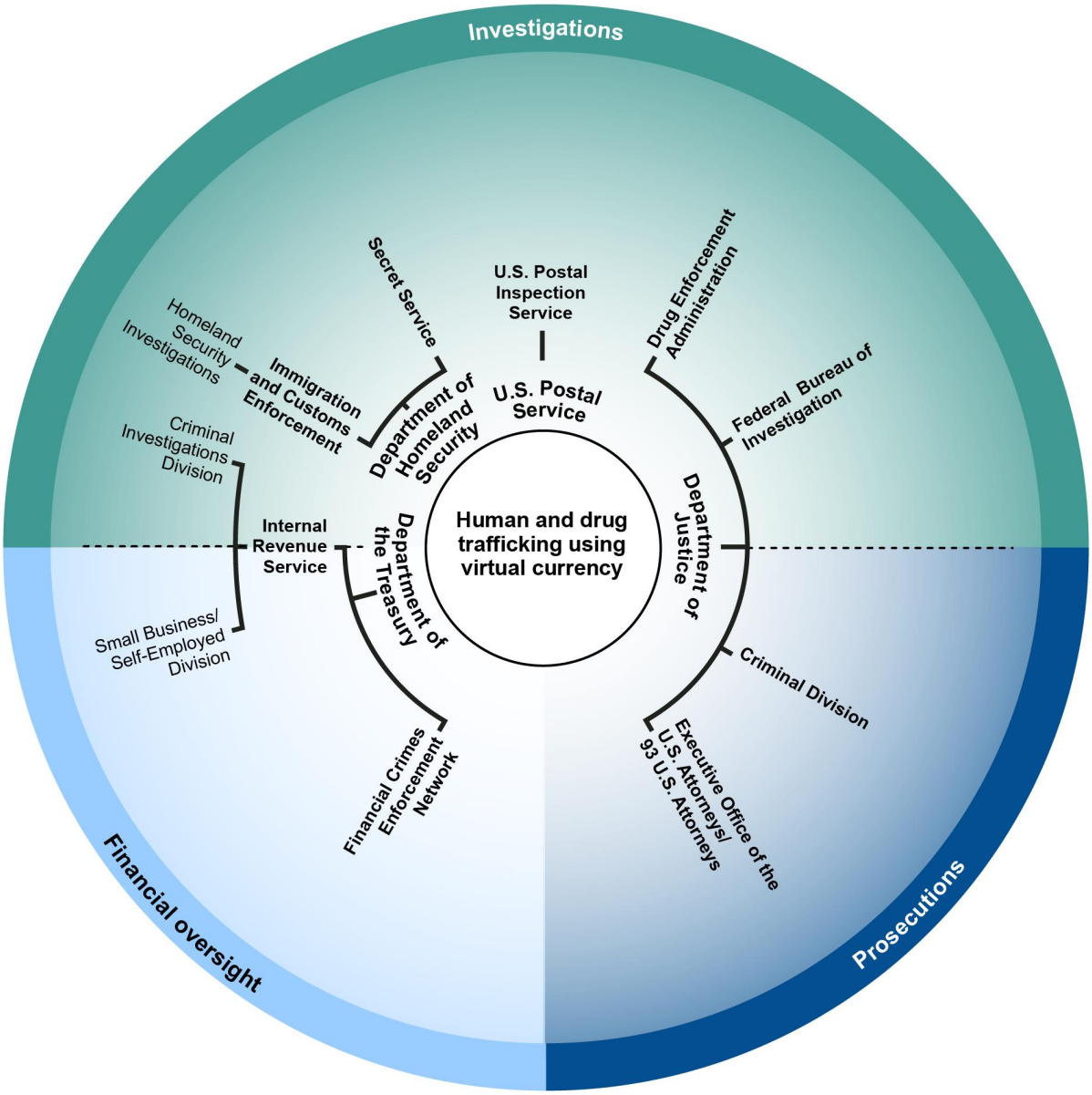
[44]FinCEN also delegated BSA/AML examination authority to the federal banking regulators, the U.S. Securities and Exchange Commission, and the Commodity Futures Trading Commission. As part of their BSA/AML roles, these agencies have certain responsibilities for some activities and products that involve virtual currencies.

[45]IRS's Small Business/Self-Employed Division conducts BSA compliance examinations of nonbank financial institutions (such as money transmitters and casinos) and refers cases to FinCEN for potential civil enforcement action or to IRS-CI if the examiners believe a criminal violation may be involved.

conjunction with human and drug trafficking cases.[46] Furthermore, the Executive Office for U.S. Attorneys provides general executive assistance and supervision to the offices of the U.S. Attorneys. These prosecutorial components often work together to target and prosecute criminal offenses either in partnership or through programmatic support and guidance.

[46]In addition, DOJ's Civil Rights Division plays a role in countering human trafficking facilitated with virtual currencies.

Figure 2: Primary Federal Agencies Involved in Countering Human and Drug Trafficking Facilitated by Virtual Currency



Source: GAO analysis of federal entities' documentation. | GAO-22-105462

Note: This illustration includes the primary federal agencies and their components involved in the oversight of virtual currency market participants—such as exchanges—as well as the investigation and prosecution of human and drug trafficking facilitated with virtual currency. Other federal components can also be involved in countering human and drug trafficking facilitated with virtual currency.

Virtual Currency Can Be Used in Human and Drug Trafficking Transactions, but Data Collected by Selected Federal Agencies May Be Incomplete

Virtual Currency Can Be Used to Facilitate Human and Drug Trafficking

Human Trafficking

Evidence suggests that virtual currency is one of several payment options used in sex trafficking but may not be as frequently used in labor trafficking.[47] The internet has enabled an online market for commercial sex, which may be used to promote the prostitution of oneself or others and sex trafficking. Some financial transactions involving sex trafficking may be entirely conducted online, such as through the sale of imagery or live virtual sex shows involving trafficked individuals. Other transactions may be initiated online, such as through advertisements where buyers can purchase sexual services provided by trafficked individuals—with services ultimately being rendered in person.[48]

Online websites that are used to promote prostitution and sex trafficking exist in the United States and abroad, which may affect thousands of adults and minors, some of whom may be victims of sex trafficking. A 2014 study conducted by the Urban Institute's Justice Policy Center, a nonprofit research organization, found online advertising was the most commonly used form of advertising among offenders convicted of crimes

[47]With regard to labor trafficking, we did not identify publications that cited the use of virtual currency in labor trafficking. Officials from the Department of Labor and other federal entities we spoke with have not identified the use of virtual currency in labor trafficking cases as a trend.

[48]Advertisements on commercial sex market platforms can include postings from traffickers, as well as individuals independently engaging in prostitution, according to Polaris. According to the Human Trafficking Institute, when a trafficker solicits a buyer online, the trafficker often transports the victim to meet the buyer—usually at a hotel—or the buyer may come to the victim. In cases not involving internet solicitation, the commercial sex acts may occur at the same location where the trafficker solicited the buyer (e.g., the street, a brothel). The Human Trafficking Institute, *2019 Federal Human Trafficking Report* (Fairfax, VA: 2020).

related to the facilitation of prostitution or sex trafficking, in eight major U.S. cities.[49] The Human Trafficking Institute, a human trafficking prevention nongovernmental organization, reported that defendants used the internet as their primary means of soliciting buyers of commercial sex in 84 percent (390 of 466) of active federal sex trafficking cases in 2019 for which the primary method of solicitation was available in public sources.[50] For example, before its seizure in 2018, backpage.com was the leader in the U.S.' online commercial sex market for several years, as noted in our June 2021 report.[51] According to a July 2020 report by Polaris, following backpage.com's seizure in 2018, some existing commercial sex market platforms shutdown or suspended services in the U.S. while other sites moved operations abroad.[52] Additionally, other commercial sex market platforms have emerged.

[49]Meredith Dank et al., *Estimating the Size and Structure of the Underground Commercial Sex Economy in Eight Major U.S. Cities* (The Urban Institute Justice Policy Center: March 2014).

[50]The Human Trafficking Institute, *2019 Federal Human Trafficking Report* (Washington, D.C.: 2019). This percentage is based on the 466 sex trafficking cases active in 2019 in which the primary method of solicitation was available in public sources. Human Trafficking Institute data are taken from federal criminal cases that involved (1) one or more charges under Chapter 77 of Title 18,U.S. Code, 18 U.S.C. §§ 1581-97 (Peonage, Slavery, and Trafficking in Persons); or (2) one or more charges under statutes outside of Chapter 77 where there was substantial evidence of force, fraud, coercion, commercial sex with a child, or an identified victim of trafficking. Human Trafficking Institute data do not reflect the prevalence of sex trafficking in the U.S. but instead represent key findings and trends in federal sex trafficking prosecutions. For each case, the Human Trafficking Institute reviewed complaints and charging instruments, key motions and briefs, plea agreements, verdict forms, sentencing memorandums, judgments, and appeal information. The case information added to the database was reviewed by the project attorneys to ensure accuracy and completeness.

[51]See GAO-21-385 for more information. Following backpage.com's seizure on April 6, 2018, 5 days later was the enactment of the Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (FOSTA), Pub. L. No. 115-164, 132 Stat. 1253, which established criminal penalties for those who control online platforms with intent to promote or facilitate the prostitution and sex trafficking of others.

[52]Polaris, *Using an Anti-Money Laundering Framework*. Polaris also stated in the 2020 report that backpage.com was involved in the majority of child trafficking reports to the National Center for Missing and Exploited Children made by the general public. Further, prior to backpage.com's seizure in April 2018, the National Human Trafficking Hotline reported that during a 4-year period (calendar years 2012 through 2016) it received over 4,000 calls, emails, or online tip reports in connection to domestic and international cases referencing the website. Almost 94 percent of victims reported were female and 41 percent of victims were minors. National Human Trafficking Hotline, *National Hotline Calls and Cases Referencing Backpage.com, United States and International: 1/1/2012-12/31/2016* (April 2018).

Federal prosecutors have brought criminal cases against the owners, managers, or operators of online commercial sex market platforms (see text box).

Examples of Cases That Involved the Use of Virtual Currency, Brought Against Owners, Managers, or Operators in the Online Commercial Sex Market

- **Backpage.com (2018):** Defendants are alleged to have accepted payment in virtual currencies such as Bitcoin and Litecoin, from traffickers who sought to advertise victims for commercial sex on backpage.com, a commercial forum. Allegations include that traffickers used virtual currency to pay for advertisements on backpage.com after credit card companies stopped processing payments on the website. The defendants are alleged to have used third-party exchanges to process virtual currency payments. The indictment details included 17 victims, five of whom were minors, and four of whom are alleged to have been killed in the course of being trafficked, including three victims allegedly murdered by customers. As of September 2021, this case, and related cases, are pending, and between $13.9 million and $16 million worth of virtual currency from four virtual currency addresses were seized and/or subject to potential forfeiture from backpage.com. (USA v. Lacey et al.; USA v. Ferrer; and USA v. Backpage.com LLC, et al)
- **Cityxguide.com (2020):** The defendant (owner and operator of platform) is alleged to have received payments of Bitcoin or gift cards from major retailers from traffickers who sought to advertise victims for commercial sex on cityxguide.com, a commercial forum. Traffickers allegedly used Bitcoin or gift cards for premium advertisement placement that increased the ad's visibility on the website. Law enforcement identified numerous minor victims that were advertised on cityxguide.com, including a 13-year old recovered in November 2019. As of September 2021, the case is pending, and while 12 bank accounts were seized and/or subject to forfeiture, it is unclear if these accounts include profits from Bitcoin payments on cityxguide.com and the estimated worth of these payments. However, since 2018, more than $21 million has allegedly been laundered from gift card payments that were exchanged through a third-party gift card reseller. (USA v. Martono)

Source: GAO analysis of court documents and information from the Department of Justice : and GAO, *Sex Trafficking: Online Platforms and Federal Prosecutions*, GAO-21-385 (Washington, D.C.: June 21, 20021). I GAO-22-105462

Payment Methods Accepted by Platforms in the Online Commercial Sex Market

According to Polaris, platforms in the online commercial sex market generally can accept a combination of the following payment methods:

- **Credit/debit cards:** Payments through credit or debit cards, including prepaid debit products.
- **Virtual currency:** Transfer of virtual currency, including platforms that use third-party wallet providers and exchanges.
- **Store-brand gift cards:** Transfer of store-brand gift cards directly to the platform site or to a separate account holder, or through a third party gift card transfer/redemption site.
- **Check/wires/money orders:** Sending checks or money orders to a specified address or wire transfers into a bank account held by the commercial sex advertising website or a separate account holder.

Source: Polaris, *Executive Summary: Using an Anti-Money Laundering Framework to Address Sex Trafficking Facilitated by Commercial Sex Advertisement Websites* July 2020. | GAO-22-105462

In June 2021, we reported on payment methods accepted by platforms in the online commercial sex market.[53] As part of that review we analyzed payment methods accepted by 27 platforms.[54] Such platforms may be used to facilitate sex trafficking. We found that over half of the platforms (15 of 27) accepted virtual currency as a form of payment (including sites that used third-party wallet providers and exchanges). Of these 15 platforms, most (11) accepted another form of payment, including credit or debit cards; checks, wires, or money orders; or store-brand gift cards. Further, three platforms only accepted virtual currency as a form of payment.[55] We found that overall, platforms in the online commercial sex market accepted a variety of traditional and alternative payment methods and utilized evasive techniques—such as the use of third parties—to facilitate illicit transactions (see sidebar). Additionally, we found that the 15 platforms that accepted virtual currency as a form of payment primarily promoted or facilitated direct, in-person sexual services or services that are seemingly legal but mask in-person sexual services that may be expected or implied.[56]

Polaris conducted a similar review of 40 platforms in the online commercial sex market and found that most websites (23 out of 40) accepted virtual currency as a form of payment.[57] According to Polaris's review, these platforms primarily accepted Bitcoin, Bitcoin Cash, Litecoin, and Ether. Further, Polaris reviewed the Bitcoin addresses for four websites, three of which received transactions that averaged between

[53]GAO-21-385.

[54]For a detailed description of our analysis, please see GAO-21-385, app. I.

[55]For one platform that accepted virtual currency, we were unable to determine if it accepted another payment method.

[56]"Direct in-person sexual services" refers to platforms that directly promote in-person sexual services. Such services are not masked as legal services and do not create the expectation of a continuing relationship. "Services that are seemingly legal" refers to platforms where the façade of services that are seemingly legal—such as massage or health/beauty services—mask the promotion of in-person sexual services that are expected or implied. For more information, see GAO-21-385.

[57]Polaris, *Using an Anti-Money Laundering Framework*. Polaris conducted its analysis from October 2019 to May 2020, Polaris stated that the online commercial sex market platforms they reviewed are platforms used by both sex traffickers and individuals independently engaging in prostitution. However, Polaris included these platforms in their review because the platforms are at risk of facilitating sex trafficking of victims, including minors.

$50 and $80 at the time of the study. The fourth site exclusively received Bitcoin payments valued at about $2,509 at the time of the study.

According to the Polaris report, one reason platforms in the online commercial sex market accept alternative payment methods—including virtual currency—may be the difficulty platforms have in maintaining reliable credit and debit card payment systems. For example, in 2015, Visa, MasterCard, and American Express stopped processing payments to backpage.com—the largest online marketplace for buying and selling commercial sex at the time—due to allegations that the website was used to promote prostitution and possible sex trafficking. The April 2019 Childsafe.ai report states that, prior to its seizure in April 2018, backpage.com had to perform "financial gymnastics" to take credit cards for advertising.[58] Specifically, constantly applying for new merchant accounts, changing billing descriptors, and spreading payments across multiple accounts (i.e. load balancing) to keep fraud/chargeback rates under acceptable limits requires significant expertise and time.[59] Although traditional payment methods are still used to facilitate human trafficking, virtual currency may be used by owners and operators of online platforms to host the site's servers and may be accepted as payment to advertise commercial sex, according to DOJ officials. Furthermore, according to ICE-HSI officials we interviewed, certain virtual currency's anonymizing features attract sex traffickers.

In addition, platforms in the online commercial sex market appear to be encouraging the use of virtual currency. For instance, some platforms offer discounted rates to customers who pay with virtual currency, according to the Polaris report. This report also states that most platforms that accept virtual currency incorporate a third-party virtual currency exchange into their payment system. This can make using virtual currency more accessible to nontechnical customers by allowing them to use traditional payment methods, such as debit cards, to obtain virtual currency and then transfer the virtual currency to the platform with relative ease.

[58]Childsafe.ai, *Beyond Backpage: Buying and Selling Sex in the United States One Year Later* (April 2019). Childsafe.ai is a software company that deploys machine learning and active collection networks to observe criminals who buy and sell human beings online.

[59]According to the childsafe.ai Chief Executive Officer, a chargeback rate for a merchant account is the number of charge disputes made against the total volume of transactions, expressed as a percentage. For more information, see GAO-21-385.

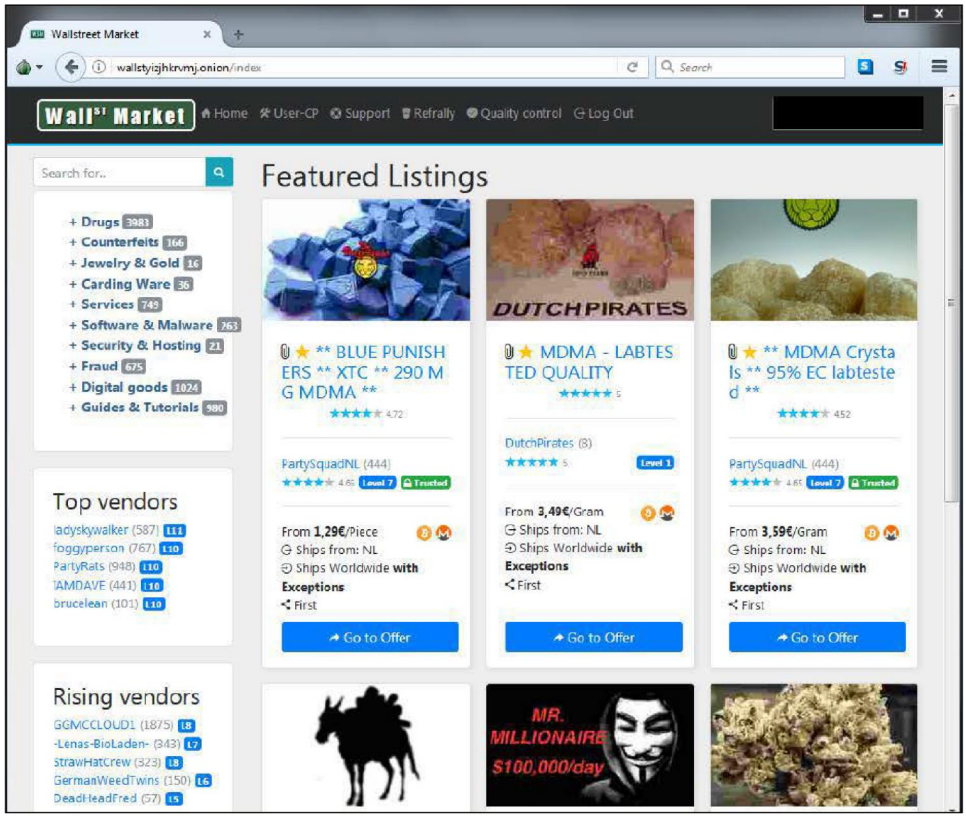
Drug Trafficking

Virtual currency has been used for the sale and purchase of illegal drugs on Dark Web marketplaces for a number of years. Officials from several federal agencies stated that drug trafficking is a common illicit use of virtual currency, as observed by these agencies. Specifically, officials from ICE-HSI's Cyber Crimes Center stated that an estimated 80 to 90 percent of Dark Web sales their agency has observed are related to illegal drugs and all are virtual currency transactions in the form of cryptocurrency because other payment types are generally not accepted on Dark Web marketplaces. According to officials from the Office of National Drug Control Policy, buyers often have relationships with a particular seller and may save their wallet on a particular seller's website. Further, officials from the Office of National Drug Control Policy stated that virtual currencies have been central to the rise of drug sales in the U.S., specifically fentanyl and other synthetic opioids.

In addition, as noted in DOJ's October 2020 *Cryptocurrency Enforcement Framework*, the increased use of virtual currency to sell and buy illegal drugs on the Dark Web and by drug cartels to launder their profits has contributed to the U.S.' drug epidemic, which, according to the U.S.'s Centers for Disease Control and Prevention, claimed over 70,600 lives in 2019 alone.[60] However, an official from ICE-HSI's Illicit Finance Proceeds of Crimes Unit stated that virtual currency can also be used to purchase illegal drugs outside of the Dark Web. For example, a drug dealer may receive virtual currency payments from a buyer and send the narcotics through the mail. Then the dealer can convert the virtual currency to cash or use it to purchase additional supplies of drugs, according to the ICE-HSI official. See figure 3 for an example of a Dark Web marketplace that accepted virtual currency to purchase illegal drugs prior to its seizure and shutdown.

[60]Department of Justice, *Cryptocurrency Enforcement Framework*; C.L. Mattson, et al., "*Trends and Geographic Patterns in Drug and Synthetic Opioid Overdose Deaths—United States, 2013-2019," Morbidity and Mortality Weekly Report*, v. 70, no. 6 (U.S. Department of Health and Human Services: Centers for Disease Control and Prevention: Feb. 12, 2021).

Figure 3: Example of Illegal Drugs Listed on Wall Street Market, a Dark Web Marketplace that was Seized and Shut Down



Source: Department of Justice. | GAO-22-105462

One of the most prominent Dark Web marketplaces was Silk Road, which came online around 2011. At the time of its seizure in 2013, Silk Road was considered the most sophisticated and extensive criminal marketplace on the internet and was used by several thousand drug dealers to distribute hundreds of kilograms of illegal drugs, according to a DOJ press release.[61] The website was designed to include a Bitcoin-based payment system to help conceal illicit transactions. In November 2020, federal agents seized virtual currency worth over $1 billion and alleged that it was comprised of proceeds from unlawful activity

[61]Department of Justice, *Manhattan U.S. Attorney Announces The Indictment of Ross Ulbricht, The Creator And Owner Of The "Silk Road" Website* (Feb. 4, 2014). In addition to illegal drugs, silkroad.com also sold a variety of illicit goods, such as malicious software; pirated content; and forged identification documents and services, such as computer hacking.

conducted on Silk Road.[62] According to DOJ officials, following the shutdown and seizure of Silk Road and AlphaBay (another prominent Dark Web marketplace), a number of smaller marketplaces have emerged, as criminals have intentionally moved their operations to smaller marketplaces to avoid detection. In addition, according to DOJ officials, 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.

Federal prosecutors have brought criminal cases against the owners, managers, or operators of some Dark Web marketplaces that facilitated the sale and purchase of illegal drugs, as well as traffickers that sold illegal drugs on Dark Web marketplaces (see text box).

[62]Department of Justice, *United States Files a Civil Action to Forfeit Cryptocurrency Valued at Over One Billion U.S. Dollars* (Nov. 5, 2020).

Examples of Cases That Involved the Use of Virtual Currency to Sell or Purchase Illegal Drugs, Brought Against Owners, Managers, or Operators of Dark Web Marketplaces or Traffickers

- **Silk Road (2014):** Silk Road had a Bitcoin-based payment system for users to sell and purchase various illegal drugs (e.g., heroin, cocaine, and methamphetamine), as well as other illicit goods (e.g. malicious software, forged identification documents) and services (e.g., computer hacking). In October 2013, federal agents arrested Silk Road's owner and seized 173,991 bitcoins, which was valued at over $150 million in February 2014. Moreover, in November 2020 federal agents seized thousands of bitcoins, worth over $1 billion at the time of seizure. Federal investigators allege that the virtual currency are proceeds from unlawful activity conducted on Silk Road. At least six overdose deaths worldwide, including two minors, have been linked to illegal drugs purchased from Silk Road. In June 2015, the court sentenced the defendant to a term of imprisonment and entered a money judgment of nearly $184 million. (USA v. Ulbricht)
- **Alphabay (2017):** Users of Alphabay, a Dark Web marketplace, allegedly sold and purchased various illegal drugs, (e.g., marijuana, cocaine, fentanyl, and methamphetamine), as well as other illicit goods (e.g., firearms, toxic chemicals) and services (e.g., money laundering) with virtual currencies, such as Bitcoin, Monero, Ether, and Zcash. The website also allegedly provided mixing and tumbling services to obfuscate virtual currency transactions on the site. Multiple overdose deaths across the U.S. have been linked to fentanyl and heroin sales from Alphabay. The July 2017 criminal indictment was dismissed in April 2018 because of the defendant's death, while a related forfeiture proceeding is pending as of September 2021, which includes approximately $8.8 million worth of virtual currencies federal law enforcement took control of from the defendant. (USA v. Cazes)
- **Wall Street Market (2019):** Users of Wall Street Market, a Dark Web marketplace, allegedly sold and purchased various illegal drugs, as well as other illicit goods (e.g., counterfeit goods) and services (e.g., computer hacking software) with virtual currencies, such as Bitcoin and Monero. Prior to the website's seizure, the website's administrators held approximately $11 million worth of virtual currency in users' escrow accounts and allegedly diverted the money into their own accounts. An individual died as a result of overdosing on a nasal spray laced with fentanyl that has been linked to a purchase through Wall Street Market. According to the Department of Justice (DOJ), the case is pending as of September 2021. (USA v. Lousee et al)
- **Buyersclub (2020):** Under the moniker "buyersclub," among others, a trafficker allegedly purchased illegal drugs, including OxyContin, morphine, and Xanax, from a third-party to sell on different Dark Web marketplaces (i.e., silkroad.com, alphabay.com) in exchange for Bitcoin. The defendant allegedly received over 23,900 bitcoins at various addresses from several Dark Web marketplaces from about December 2012 to about July 2020, worth approximately $270 million at the time of the indictment, which may have worth a different value at the time of the transactions. No overdose deaths have been identified as a result of purchasing illegal drugs through this trafficker, as of September 2021. According to DOJ, the case is pending as of September 2021. (USA v. Pate)

Source: GAO analysis of court documents and information from the Department of Justice. I GAO-22-105462

Whether using virtual currency to purchase illegal drugs through direct contact with a seller or online through a Dark Web marketplace, illegal drugs can be delivered to individuals using the postal and courier systems. For example, in February 2021, two individuals were arrested

and charged for allegedly selling counterfeit Adderall pills that contained methamphetamine on a Dark Web marketplace in exchange for Bitcoin and used a postage reseller to ship the pills to buyers, according to DOJ documents.[63] Postal Inspection Service officials also noted that the majority of illicit drug transactions their agency comes across are domestic shipments, regardless of payment type. They noted that the types of illegal drugs purchased with virtual currency on the Dark Web and seized by the Postal Inspection Service are consistent with the types of drugs the Postal Inspection Service has seized through other means.[64]

Drug cartels and transnational criminal organizations can also use virtual currencies to launder their trafficking profits. For example, DOJ and Postal Inspection Service officials stated that drug cartels and 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. According to the DEA's 2020 National Drug Threat Assessment, while preferred methods to move and launder illicit proceeds have largely remained the same throughout the years (e.g., bulk cash smuggling and trade-based money laundering), virtual currency is becoming more commonly used by international money launderers to transfer proceeds across borders on behalf of transnational criminal organizations.[65] Specifically, there has been evidence of Mexican and Colombian transnational criminal organizations using virtual currencies to transfer proceeds internationally, according to the National Drug Threat Assessment. For example, money couriers deposit large volumes of cash from illegal drug proceeds into a kiosk to convert the value to virtual currency. Once the illicit proceeds are in this form, the funds can easily be transferred to another virtual currency user's wallet, reducing the risk associated with transporting bulk currency. Illegal drug proceeds may also be converted from virtual currency to fiat currency such as the U.S. dollar. Secret Service officials told us that transnational criminal organizations establish money courier networks and leverage illicit exchange networks, as well as the Dark Web, to exchange illicitly

[63]USA v. Ombisi, No. 2:21-cr-20011, Doc. 1, Complaint (Filed Feb. 9, 2021).

[64]Generally, according to Postal Inspection Service officials, the U.S. Postal Inspection Service has seized more methamphetamine and cocaine, while opioids, including fentanyl, comprised a small portion of seizures (less than 5 or 10 percent).

[65]Drug Enforcement Administration, *2020 National Drug Threat Assessment* (March 2021).

gained virtual currency for fiat currency, and reversely, fiat currency for virtual currency.

The Use of Virtual Currency in Human and Drug Trafficking Appears to be Increasing, but Inconsistencies in Selected Federal Agencies' Data Collection Methods May Yield Incomplete Data

A significant limitation to accurately understanding the extent of human and drug trafficking activities is that perpetrators of these illicit activities are purposefully trying to hide, or obfuscate, their actions, making it difficult to fully account for the number of criminal violations. Adding the use of virtual currency into the mix, which can be used to purposely conceal financial transactions related to illicit activity, further complicates efforts to account for or develop reliable estimates. Nevertheless, data collected by federal financial regulators and law enforcement agencies provide some insight on the use of virtual currency in human and drug trafficking.

Financial institutions are required to file Suspicious Activity Reports (SAR) with FinCEN if they know, suspect, or have reason to suspect that a transaction may involve illicit activity.[66] FinCEN is responsible for collecting, analyzing, and disseminating financial intelligence information received from financial institutions–such as banks and virtual currency exchanges. Information collected by FinCEN indicates that the use of virtual currency in financial activity connected to human and drug trafficking is increasing. For example, the number of SARs financial institutions filed to FinCEN that referenced virtual currency terms quadrupled during a 4-year period from 10,377 in calendar year 2017 to 42,782 in calendar year 2020.[67] In calendar years 2017 through 2020, the number of SARs financial institutions filed that referenced both virtual

[66]Under FinCEN regulation, banks and MSBs are required to file this type of report when (1) a transaction involves or aggregates at least $5,000 in funds or other assets for banks or at least $2,000 in funds or other assets for MSBs and (2) the institution knows, suspects, or has reason to suspect that the transaction is suspicious. See 31 C.F.R. §§ 1020.320 (Reports by Banks) 1022.320 (Reports by MSBs).

[67]According to FinCEN officials, this increase may be due, in part, to financial institutions improving their methods to identify and report potential illicit activity that involves virtual currency.

currency and human trafficking almost doubled, from 36 to 68.[68] Further, the number of virtual currency SARs identifying drug trafficking-related activity increased by more than fivefold from 252 in calendar year 2017 to 1,432 in calendar year 2020.[69] While the filing of a SAR is not a clear indication that a crime has occurred, it is an indicator of potentially illicit activity.

Law enforcement agencies, such as DHS, DOJ, IRS, and the Postal Inspection Service, have also collected some data on the use of virtual currency in human or drug trafficking cases. For example, during the same 4-year period, IRS identified six investigations that involved virtual currency that were also associated with human trafficking—specifically sex trafficking. Similarly, ICE-HSI had one investigation that involved virtual currency and human trafficking. For the agencies we reviewed, many cases that involved virtual currency from fiscal year 2017 through 2020 were associated with drug trafficking. For example, among ICE-HSI's investigations that involved virtual currency during this period, about 36 percent (366 of 1,009) involved drug trafficking.[70] Similarly, among IRS's investigations about 25 percent (48 of 194) involved drug trafficking.[71] Further, 85 percent of the Postal Inspection Service's seizures of virtual currency involved drug trafficking (142 of 167).[72]

However, a number of data capture shortfalls at these agencies and others may limit the completeness and accuracy of available data on the

[68]Since 2018, FinCEN's SAR form has included a checkbox for filers to flag if the financial activity is associated with human trafficking. FinCEN's summary data for calendar year 2017 were generated by querying narrative data, and summary data for calendar years 2018 through 2020 were produced by summing the number of SARs that selected the human trafficking check-box.

[69]To arrive at this figure, FinCEN officials told us they searched narrative SAR data for common payment methodologies associated with drugs, such as trade-based money laundering, and other controlled substance terms, such as drugs, narcotics, fentanyl, and names of cartels.

[70]During this period, the number of ICE-HSI investigations that involved both virtual currency and drug trafficking increased from 55 to 89.

[71]During this period, the number of IRS-CI investigations that involved both virtual currency and drug trafficking increased from 11 to 16.

[72]During this period the number of DEA investigations that involved both virtual currency and drug trafficking increased from 40 to 74. During the same period the number of Postal Inspection Service seizures of virtual currency related to drug trafficking increased from six to 33.

presence of virtual currency, human trafficking, and drug trafficking. In general, we found that data from selected federal agencies on virtual currency use for human and drug trafficking may not be consistently captured.[73] Consequently, agencies may lack complete data when assessing or reporting on the illicit use of virtual currency in human trafficking or the illicit use of virtual currency in drug trafficking. As a result, in the sensitive version of this report, we made nine recommendations to selected agencies to enhance their data collection practices.[74] Our sensitive report described the extent to which each agency had methods and system controls in place for consistently collecting data on the presence of virtual currency, human trafficking, and drug trafficking and identified shortcomings related to the information agencies collect, along with causes of the shortcomings. Discussion of these methods, system controls, shortcomings, and related causes have been omitted from this report because the information was deemed sensitive by DOJ.

Selected Federal Agencies Help Counter the Illicit Use of Virtual Currency in Human and Drug Trafficking, but Face Oversight and Technology Challenges

Selected Agencies Leverage Various Criminal Statutes and Anti-Money Laundering Regulations to Counter the Use of Virtual Currency in Human and Drug Trafficking

Law enforcement agencies use existing criminal statutes that relate to the underlying criminal activity, such as human and drug trafficking, as the legal basis to pursue investigation and prosecution of individuals and

[73]These agencies include ICE-HSI, Secret Service, DEA, FBI, DOJ's Criminal Division, DOJ's Justice Management Division, IRS Criminal Investigations, FinCEN, and the Postal Inspection Service.

[74]In GAO-21-104129SU, the sensitive version of this report, we recommended that, to the extent practicable, FinCEN, ICE-HSI, Secret Service, DEA, FBI, DOJ's Criminal Division, DOJ's Justice Management Division, IRS Criminal Investigations, and the Postal Inspection Service, identify and employ improved methods to consistently capture data on the use of virtual currency in human and drug trafficking. All but one agency, DHS's ICE-HSI, concurred with the recommendation.

businesses who use virtual currency in furtherance of criminal activity. Law enforcement agencies also use information collected as required by BSA/AML regulations to detect and investigate criminal activity involving virtual currency. In addition, the AML Act amended relevant BSA/AML definitions to make anti-money laundering enforcement authorities explicitly applicable to value substituting for currency.[75]

Law Enforcement

Federal law enforcement agencies pursue criminal investigations and prosecutions for human and drug trafficking-related illicit conduct, including those using virtual currency, under various statutes that pertain to the alleged criminal conduct, such as the following U.S. Code provisions:

- Sex Trafficking, 18 U.S.C. § 1591
- Forced Labor, 18 U.S.C. § 1589
- Drug Trafficking, 21 U.S.C. § 841
- Promotion or Facilitation of Prostitution/Trafficking, 18 U.S.C. § 2421A
- Mail Fraud, 18 U.S.C. § 1341
- Money Laundering, 18 U.S.C. § 1956
- Transactions Involving Proceeds of Illegal Activity, 18 U.S.C. § 1957
- Operation of an Unlicensed Money Transmitting Business, 18 U.S.C. § 1960
- Interstate and Foreign Travel or Transportation in Aid of Racketeering Enterprises, 18 U.S.C. § 1952
- Racketeer Influenced and Corrupt Organizations (RICO), 18 U.S.C. ch. 96 (§§ 1961-1968)

[75]See 31 U.S.C. §§ 5312(a), 5330(d).

Alphabay

On July 20, 2017, the Department of Justice announced the seizure of Alphabay, a large Dark Web marketplace used to buy and sell illegal goods and launder hundreds of millions of dollars' worth of virtual currency deriving from these illegal transactions. According to the indictment, Alphabay required its users to transact only in digital currencies. Law enforcement authorities in the U.S. worked with numerous foreign partners to freeze and preserve millions of dollars' worth of virtual currency that were the subject of forfeiture counts in the indictment and that represent the proceeds of the Alphabay organization's illegal activities. Criminal charges included, among others, narcotics conspiracy, distribution of a controlled substance, money laundering conspiracy and criminal forfeiture.

Source: GAO analysis of U.S Department of Justice press release, number 17-803. | GAO-22-105462

For example, in June 2020, federal prosecutors charged the operator of cityxguide.com with promotion and facilitation of prostitution and reckless disregard of sex trafficking, racketeering, and money laundering.[76] In addition, in April 2018, federal prosecutors charged seven individuals associated with backpage.com with crimes including facilitating prostitution and money laundering.[77]

Federal prosecutors may bring money laundering and other financial crimes charges in cases involving sex or labor trafficking, and drug trafficking, including where virtual currency is used. According to DOJ's *Cryptocurrency Enforcement Framework*, a publication produced by the Attorney General's Cyber-Digital Task Force, criminals of all types are increasingly using cryptocurrency to launder their illicit proceeds.[78] Federal prosecutors have brought money laundering charges in cases potentially involving promotion of sex trafficking, including where virtual currency was used, such as the cityxguide.com and backpage.com cases described above. In addition, several administrators and operators of Dark Web marketplaces, such as Alphabay (see sidebar), Wall Street Market, and Dream Market, that offered the sale of illegal goods, were charged with drug trafficking-related crimes and money laundering, among other charges.[79]

Companies engaged in the money transmission of virtual currencies may also risk noncompliance with BSA requirements if they are deemed to be

[76]Department of Justice, *U.S. Attorney's Office Shuts Down Website Promoting Prostitution and Sex Trafficking, Indicts Owner* (June 19, 2020).

[77]Department of Justice, *Justice Department Leads Effort to Seize Backpage.Com, the Internet's Leading Forum for Prostitution Ads, and Obtains 93-Count Federal Indictment* (April 9, 2018).

[78]Department of Justice, *Attorney General's Cyber Digital Task Force, Cryptocurrency Enforcement Framework* (Washington D.C.: October 2020). The DOJ report provides an overview of the emerging threats and enforcement challenges associated with the increasing prevalence and use of cryptocurrency; details the relationships that the Department of Justice has built with regulatory and enforcement partners both within the U.S. government and around the world; and outlines the department's response strategies.

[79]In October 2018, an administrator of the Dark Web marketplace, Dream Market, was sentenced to 20 years in federal prison for narcotics trafficking and money laundering. In May 2019, charges in Wall Street Market included conspiracy to launder monetary instruments, and distribution and conspiracy to distribute controlled substances.

operating as an unlicensed money transmitter.[80] For example, in 2017, BTC-e, a digital currency exchange, and its operator were charged with operating an unlicensed money services business and money laundering.[81] In addition, on July 22, 2020, DOJ announced that a California man agreed to plead guilty to operating an illegal money services business, called Herocoin, that exchanged between $15 million and $25 million, including proceeds for criminal activity, through in-person exchanges and transactions occurring at his virtual currency kiosks (also called "Bitcoin ATMs").[82] The defendant intentionally failed to register Herocoin with FinCEN and admitted that he was aware of, but chose not to comply with, requirements to develop and maintain an effective anti-money laundering program, among other BSA requirements.

Using the criminal and civil forfeiture statutes, law enforcement agencies have also seized and sought forfeiture of virtual assets and other property derived from or involved in human and drug trafficking offenses.[83] For example, between $13.9 million and $16 million worth of virtual currency from four virtual currency addresses were seized and/or subject to potential forfeiture from backpage.com. Further, the creator and administrator of Alphabay had numerous high-value assets seized by the FBI and DEA, including millions of dollars in virtual currency. Similarly, in the case of BTC-e and its operator, law enforcement seized property involved with operating an unlicensed money services business, money laundering, and activities related to engaging in unlawful monetary transactions.

[80]See, generally, 31 C.F.R. pt. 1022, in particular, § 1022.380 (Registration of Money Service Businesses).

[81]The indictment alleges that BTC-e facilitated transactions for cybercriminals worldwide, including narcotics distribution rings. The Department of Justice filed criminal charges against BTC-e and its operator, including for money laundering offenses (18 U.S.C. §§ 1956, 1957) and operating as an unlicensed money services businesses (18 U.S.C. § 1960). In addition, FinCEN assessed a $110 million civil penalty against the exchange for willfully violating U.S. anti-money laundering laws, and a $12 million penalty against the exchange's operator personally.

[82]Department of Justice, U.S. Attorney's Office, Central District of California, *O.C. Man Admits Operating Unlicensed ATM Network that Laundered Millions of Dollars of Bitcoin and Cash for Criminals' Benefit* (Los Angeles, CA.: July 22, 2020).

[83]Criminal forfeiture: see, e.g., 18 U.S.C. §§ 982, 2253; 21 U.S.C. § 853, 881; civil forfeiture: see, e.g., 18 U.S.C. §§ 981, 983-985; 21 U.S.C. § 881.

Federal Regulators

Federal agencies regulate and oversee virtual currency entities. For example, FinCEN defines virtual currency exchangers as money transmitters for the purposes of the BSA.[84] Virtual currency exchangers must register with FinCEN, keep records—such as customer identification information, and make reports—such as SARs.[85] This information can be used by regulators and law enforcement to detect, investigate, and deter illicit finance activity such as human and drug trafficking. Officials from all law enforcement agencies we spoke with told us that BSA information is critical to identifying criminals using virtual currency.

The AML Act has amended definitions throughout the BSA to explicitly include "value that substitutes for currency" (i.e., virtual currency) as it relates to money transmission and money transmitters.[86] A person, regardless of their location, doing business as a money transmitter wholly or in substantial part in the U.S., such as by engaging in virtual currency transactions with U.S. customers, must register as an MSB and comply with BSA/AML requirements.[87] Such a person is also therefore subject to

[84]*See* Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*.

[85]*See* Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*.

[86]See 31 U.S.C. §§ 5312(a), 5330(d). This is consistent with FinCEN's *2011 MSB Final Rule* that, among other things, defined "money transmission services" to include accepting from one person and transmitting to another location or person, "currency, funds, or other value that substitutes for currency by any means." *See* Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses, 76 Fed. Reg. 43,585 (2011) (codified at 31 C.F.R. pts. 1010, 1021 & 1022); in particular, see 31 C.F.R. § 1010.100(ff)(5)(i)(A).

[87]In general, whether a person qualifies as an MSB subject to BSA regulation depends on the person's activities and not its formal business status. Thus, whether a person is an MSB will not depend on whether the person: (a) is a natural person or legal entity; (b) is licensed as a business by any state; (c) has employees or other natural persons acting as agents; (d) operates at a brick-and-mortar branch, or through mechanical or software agents or agencies; or (e) is a for profit or nonprofit service. FinCEN's MSB rule covers any "person" engaged in money transmission as a business, regardless of whether they are formed or registered as an entity. See generally 31 C.F.R. pt. 1022.

supervision and compliance examinations.[88] Virtual currency exchanges and administrators that are considered MSBs must

- register with FinCEN;[89]
- design and implement an effective, written, and risk-based AML program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities;[90]
- report transactions in currency over $10,000;[91]
- detect and report a suspicious transaction if it involves or aggregates funds or other assets of at least $2,000, and the MSB knows, suspects or has reason to suspect the transaction involves use of the business to facilitate criminal activity (e.g., human and drug trafficking) among other illicit purposes;[92] and
- verify customer identification and obtain and retain customer information—including the name, Social Security number, and address of the sender—if that person is not an established customer, for all transfers in the amount of $3,000 or more (see sidebar).[93]

[88]See 31 U.S.C. § 5318(a)(3). FinCEN oversees the administration of the Bank Secrecy Act and related AML regulations, and has authority to enforce BSA, including through civil monetary penalties. As the lead BSA regulator, FinCEN issues implementing regulations and ensures compliance with BSA.

[89]See 31 C.F.R. § 1022.380

[90]See 31 C.F.R. § 1022.210

[91]See 31 C.F.R. § 1010.310 and 1010.313

[92]See 31 C.F.R. § 1022.320

[93]See 31 C.F.R. § 1010.410(e)

Recordkeeping and Identity Verification Requirements

Virtual currency money transmitters are subject to Bank Secrecy Act (BSA) record-keeping and identify verification requirements. Under current requirements, virtual currency money transmitters are required to obtain and retain specified information for all transfers in the amount of $3,000 or more, including

- verifying customer identification (such as examining a state-issued identification or driver's license) when a transaction is conducted in-person and the sender is not an established customer;
- recording certain specified customer and transaction information (such as the name and address of the person placing the payment order, as well as the person's Social Security number, if that person is not an established customer);
- providing certain information to the receiving money transmitter or other receiving financial institution; and
- maintaining the record for 5 years from the date of transaction.

FinCEN proposed rules in October 2020 to update these requirements, including a proposal to lower the applicable threshold from $3,000 to $250 for international transactions and to further clarify that those regulations apply to transactions involving virtual currencies.

Source: GAO analysis of BSA regulations and FinCEN notice of proposed rulemakings. | GAO-22-105462

FinCEN has proposed rules that would update customer identification and collection requirements, by imposing verification and collection of customer information at lower thresholds and increased reporting of certain virtual currency transactions. See appendix III for more information on these proposed rules.

FinCEN has also issued recent guidance and advisories to address human and drug trafficking and clarify BSA/AML obligations for virtual currency entities, including the following:

- *Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity.* In October 2020, FinCEN issued an advisory on identifying and reporting human trafficking that provided further guidance to financial institutions on key identifiers of human trafficking, including trafficking that may be facilitated using virtual currencies on online websites.[94]
- *Advisory to Financial Institutions on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids.* This advisory was issued in August 2019 to financial institutions to help them identify illicit financial schemes and methods related to the trafficking of fentanyl and other synthetic opioids, including methodologies on how criminals use virtual currency to purchase fentanyl in online markets and anonymize their transactions.[95]
- *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies.* This May 2019 guidance clarified the application of the BSA to virtual currency businesses models such as peer-to-peer exchangers, virtual currency kiosks (also known as crypto-ATMs), privacy coins, and decentralized exchanges.[96]
- *Advisory on Illicit Activity Involving Convertible Virtual Currency.* FinCEN issued this advisory simultaneously with the Application of

[94]Financial Crimes Enforcement Network, *Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity*, FIN-2020-A008 (Oct. 15, 2020).

[95]Financial Crimes Enforcement Network, *Advisory to Financial Institutions on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids*, FIN-2019-A006 (Aug. 21, 2019).

[96]Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies,* FIN- 2019-G001 (May 9, 2019).

FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies to assist financial institutions in identifying and reporting suspicious activity related to criminal exploitation of virtual currency. For example, they identified methods, such as the use of virtual currency kiosks to convert cash to Bitcoin, then using the Bitcoin as a form of payment on Dark Web marketplaces for drug transactions.[97]

Other tools and mechanisms Treasury uses to gather information on, and prevent illicit virtual currency transactions, include Office of Foreign Assets Control (OFAC) sanctions.[98] In addition, FinCEN can leverage information-sharing statutes such as Patriot Act section 314(b) and the FinCEN Exchange.

- **OFAC sanctions.** OFAC can use financial sanctions to target criminal and other malicious actors abusing virtual currencies.[99] Firms, among other U.S persons and those subject to OFAC jurisdiction, that facilitate or engage in online commerce or process transactions using virtual currency are responsible for ensuring that they do not engage in unauthorized transactions prohibited by OFAC sanctions, such as dealings with blocked persons or property.[100] OFAC has taken two enforcement actions in the form of settlements with companies for

[97]Financial Crimes Enforcement Network, *Advisory on Illicit Activity Involving Convertible Virtual Currency*.

[98]The Office of Foreign Assets Control administers and enforces economic and trade sanctions based on national security and foreign policy priorities.

[99]Within OFAC, the Office of Compliance and Enforcement conducts civil enforcement investigations of U.S. economic sanctions violations for both fiat and virtual currency transactions.

[100]*See* Department of the Treasury, *Frequently Asked Questions, Questions on Virtual Currency, 560. Are my OFAC compliance obligations the same, regardless of whether a transaction is denominated in digital currency or traditional fiat currency?* https://home.treasury.gov/policy-issues/financial-sanctions/faqs/560, accessed July 20, 2021. According to this FAQ, the obligations are the same, regardless of whether a transaction is denominated in digital currency or traditional fiat currency. U.S. persons (and persons otherwise subject to OFAC jurisdiction) must ensure that they block the property and interests in property of persons named on OFAC's Specially Designated Nationals and Blocked Persons List or any entity owned in the aggregate, directly or indirectly, 50 percent or more by one or more blocked persons, and that they do not engage in trade or other transactions with such persons.

apparent violations of multiple sanctions programs related to digital currency transactions.[101]

OFAC administers sanctions programs that may target human trafficking, drug trafficking, and illicit activity involving virtual currency. The Global Magnitsky Sanctions program targets persons engaged in certain human rights abuses or corrupt acts around the world, and the Transnational Criminal Organizations Sanctions program can be directed against human trafficking networks with a nexus to significant transnational criminal organizations.[102] OFAC also administers the Counter Narcotics Trafficking Sanctions program that targets drug trafficking, pursuant to Executive Order 12978 and the Foreign Narcotics Kingpin Designation Act.[103] OFAC has publicly identified digital currency addresses of designated persons on its sanctions list, known as the Specially Designated Nationals and Blocked Persons List, related to fentanyl trafficking, as part of the designation of individuals tied to the Zheng Drug Trafficking Organization in August 2019.[104] The related Treasury press release stated that the drug trafficking organization used digital currency to launder proceeds from fentanyl trafficking.[105]

- **Section 314(b) information sharing.** Section 314(b) of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) allows for information sharing among financial institutions and

[101]Department of the Treasury, *OFAC Enters Into $98,830 Settlement with BitGo, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions* (Dec. 30, 2020); and *OFAC Enters Into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions* (Feb. 18, 2021).

[102]31 C.F.R. pts. 583, 590.

[103]See 31 C.F.R. pts. 536, 598; Pub. L. No. 106-120, title VIII, 113 Stat. 1606, 1626-36 (1999); Blocking Assets and Prohibiting Transactions With Significant Narcotics Traffickers, Exec. Order No. 12978, 60 Fed. Reg. 54,579 (Oct. 24, 1995) (issued Oct. 21).

[104]OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called “Specially Designated Nationals.” Their assets are blocked, and U.S. persons are generally prohibited from dealing with them.

[105]Department of the Treasury, *Treasury Targets Chinese Drug Kingpins Fueling America’s Deadly Opioid Crisis* (Aug. 21, 2019).

includes a safe harbor provision that offers protections from liability.[106] According to FinCEN's 314(b) guidance, these provisions help financial institutions to better identify and report activities that may involve money laundering or terrorist activities—such as the laundering of illicit proceeds from human and drug trafficking. On December 10, 2020, FinCEN updated this guidance to clarify the breadth of what information sharing is covered under the safe harbor provisions.[107] Participation in information sharing pursuant to Section 314(b) is voluntary, and FinCEN strongly encourages financial institutions to participate. Officials from FinCEN's Strategic Operations Division noted that some virtual currency entities participate in this program.

- **FinCEN Exchange.** Established in 2017 as an information-sharing public-private partnership on illicit finance threats, FinCEN Exchange enables financial institutions to better identify virtual currency risks and improve reporting of critical information regarding illicit virtual currency activity to FinCEN and law enforcement. The AML Act statutorily established the FinCEN Exchange program.[108] In addition to hosting FinCEN Exchanges on specific topics of illicit financial activity, FinCEN has hosted a FinCEN Exchange specifically on virtual currency. In May 2019, FinCEN hosted representatives from virtual currency money transmitters and other MSBs; third-party service providers; federal government agencies including law enforcement; and several depository institutions to discuss the threats and opportunities presented by virtual currency. Discussion topics at the exchange included methods to increase public-private collaboration and efficiency, best practices for BSA compliance and reporting, and initiatives and challenges facing the private sector related to AML and countering terrorist financing.

[106]The safe harbor provision protects from liability financial institutions or associations that transmit, receive, or share information regarding individuals, entities, organizations, and countries suspected of possible terrorist or money laundering activities for the purposes of identifying and reporting such activities. Pub. L. No. 107-56, title III, subtitle A, § 314(b), 115 Stat. 272, 308 (codified, as amended, at 31 U.S.C. § 5311 note).

[107]Financial Crimes Enforcement Network, *FinCEN Director Emphasizes Importance of Information Sharing Among Financial Institutions* (Dec. 10, 2020).

[108]Pub. L. No. 116-283, div. F, title LXI, § 6103, 134 Stat. at 4553-55 (classified at 31 U.S.C. § 310(d)).

Selected Agencies Coordinate to Counter the Use of Virtual Currency in Human and Drug Trafficking

Federal agencies participate in interagency coordination, such as task forces, deconfliction, and training, which encourages awareness and expertise in investigating, dismantling, and deterring the use of virtual currency in human and drug trafficking. Agencies work together to leverage expertise and investigate and prosecute criminals. For example, according to officials from DOJ's Computer Crime and Intellectual Property Section, they provide technical expertise relevant to electronic evidence on investigations, such as handling virtual currency on seized hardware, to other DOJ components, such as the Narcotic and Dangerous Drug Section and U.S. Attorney's offices. These officials also stated that they conducted a substantial amount of work related to Dark Web marketplaces used to traffic illegal drugs and other contraband. Similarly, ICE-HSI's Cyber Crimes Center provides expertise for cybercrime cases involving virtual currency, such as Dark Web marketplaces used for drug trafficking. They do so by providing oversight and coordination of cyber-related investigations and a range of forensic, intelligence, and investigative support services across all ICE-HSI programmatic areas. Additionally, according to DHS officials, ICE-HSI's Child Exploitation Investigations Unit and the Center for Countering Human Trafficking work together to identify and investigate operators, managers, and owners of websites that facilitate or promote sex trafficking or the distribution of child sex abuse material.[109]

[109]In October 2020, DHS established the Center for Countering Human Trafficking, an ICE-HSI-led center that integrates DHS investigative and enforcement operations, victim assistance, intelligence, outreach, and training to effectively respond to human trafficking on a global scale. The center's mission is to serve at the forefront of DHS's unified global efforts to counter human trafficking, including both sex trafficking and forced labor, through innovative law enforcement programs, education, and victim advocacy. The center accomplishes this by integrating the efforts of 16 agencies and offices from across the department and establishing an organizational mechanism to harmonize, leverage, centralize, and coordinate its capabilities and resources.

Operation Disarray

On April 3, 2018, members of the Joint Criminal Opioid Darknet Enforcement (JCODE) task force, including Department of Justice (DOJ), Federal Bureau of Investigation (FBI), and U.S. Postal Inspection Service, announced the results of Operation Disarray. Operation Disarray targeted sellers and buyers of opioids and cocaine on the Dark Web. The operation led to eight arrests and seizures of drugs, weapons, counterfeit currency, and computer equipment. Agents conducted over 160 interviews nationwide of people who bought or sold opioids and other drugs online

Operation SaboTor

On March 26, 2019, members of JCODE announced the results of Operation SaboTor, JCODE's second coordination action that involved both U.S. and international law enforcement agencies aimed at making a global impact on the opioid epidemic. The operation was a collaborative effort across JCODE entities, including the FBI, Drug Enforcement Administration, Immigration and Customs Enforcement-Homeland Security Investigations, Customs and Border Protection, Postal Inspection Service, DOJ, and Department of Defense, with participation from international partners. Law enforcement executed 65 search warrants, seizing 299.5 kilograms of drugs, 51 firearms, and more than $7 million ($4.5 million in cryptocurrency, $2.48 million in cash, and $40,000 in gold). Additionally, law enforcement made 61 arrests and shut down 50 Dark Web accounts.

Source: GAO analysis of Attorney General's Cyber Digital Task Force, Cryptocurrency Enforcement Framework. | GAO-22-105462

Agencies also participate in interagency task forces compromised of agencies across law enforcement, the intelligence community, regulators, the Department of Labor, and the Department of Defense. Agency officials we spoke with identified the following team and three task forces as important to supporting the investigation and prosecution of human and drug trafficking crimes that involve virtual currency.

- **President's Interagency Task Force to Monitor and Combat Trafficking in Persons** is a cabinet-level entity created by the Trafficking Victims Protection Act of 2000. According to the Department of State, the task force consists of 20 agencies across federal government responsible for coordinating U.S. government-wide efforts to combat trafficking in persons. Member agencies include, among others, the Department of State, Treasury, the Department of Defense, DOJ, DHS, the Department of the Interior, Department of Labor, and the Department of Transportation. On October 7, 2020, the Departments of State and the Treasury, on behalf of the President's Interagency Task Force to Monitor and Combat Trafficking in Persons, submitted an analysis of anti-money laundering efforts of the U.S. government, U.S. financial institutions, and international financial institutions related to human trafficking and recommendations to strengthen those efforts.[110] For example, one of the recommendations stated that training programs at financial institutions could focus on how to identify transactions, a series of transactions, or patterns of activity by their customers that may be indicators of human trafficking and indicators associated with virtual assets.
- **Joint Criminal Opioid Darknet Enforcement (JCODE)** is an FBI-led team. It coordinates government efforts to detect, disrupt and dismantle major criminal enterprises reliant on the Internet, the Dark Web, and other advanced technologies to traffic narcotics, weapons, and illicit services. JCODE has, for example, led the coordination of Operation Disarray and Operation SaboTor, which aimed at disrupting online drug trade on the Dark Web (see sidebar). Member agencies include DEA; the Postal Inspection Service; ICE-HSI; Customs and Border Protection; FinCEN; the Bureau of Alcohol, Tobacco, Firearms and Explosives; the Department of Defense; and DOJ.
- **Organized Crime Drug Enforcement Task Forces** is an independent component of DOJ led by the Executive Office of the

[110]National Defense Authorization Act for Fiscal Year 2020, (Pub. L. No. 116-92, div. F, title LXXI, subtitle B, § 7154(a), 133 Stat. 1198, 2259-60 (2019).

Organized Crime Drug Enforcement Task Forces. It is dedicated to disrupting and dismantling large-scale narcotics trafficking, money laundering, and high-priority transnational organized crime networks. Key member agencies include DOJ, DHS, Treasury, the Postal Inspection Service, the Department of Labor, and state and local law enforcement agencies. According to task force officials, as of September 23, 2020, approximately 6 percent of Organized Crime Drug Enforcement Task Forces' investigations involve the use of virtual currency by transnational criminal organizations engaged in sex, labor, and drug trafficking or money laundering for those criminal offenses.

- **National Cyber Investigative Joint Task Force** is an FBI-led task force that serves as a multiagency cyber center and national focal point for coordinating government-wide cyber investigations and campaigns targeting nation-state adversaries and criminal cyber organizations.[111] According to task force officials, capabilities required to trace Bitcoin and other virtual currency addresses back to real-world identities are spread across government, industry, and academia. As a result, the task force created a virtual currency team to leverage legal authorities, capabilities, and the resources of these groups to identify investigative leads and intelligence to support ongoing operations and investigations. While the task force does not lead coordination efforts specific to human and drug trafficking, it leads virtual currency coordination efforts such as bimonthly meetings with subject-matter experts across government agencies and hosts an annual virtual currency symposium.[112] According to task force officials, member agencies that have a role in virtual currency-related efforts include the FBI, DEA, the Secret Service, the Postal Inspection Service, Army Criminal Investigation Command, Treasury, and the Federal Deposit Insurance Corporation.

In addition to participating in interagency task forces, federal agencies also utilize web-based applications to conduct deconfliction and share

[111]National Security Presidential Directive-54/Homeland Security Presidential Directive-23 established the National Cyber Investigative Joint Task Force in January 2008.

[112]The Virtual Currency Symposium is 3-day annual event that is hosted by the FBI's National Cyber Investigative Joint Task Force's virtual currency team to discuss patterns and trends emerging within the virtual currency realm. This conference included discussions with domestic (federal, state, local) and foreign partner agencies. Additionally, the symposium includes engagement with industry representatives, to include exchanges and commercial tool providers, as well as academia.

evidence related to the illicit use of virtual currency.[113] For example, according to JCODE officials, the team uses DEA's Deconfliction & Information Coordination Endeavor, and DEA's Analyst and Response Tracking System, to deconflict cases and coordinate among investigators both domestically and internationally.

Federal agencies also conduct internal training and share educational materials within and across agencies to maintain and grow expertise related to virtual currency investigations and trafficking. For example, in 2017, DOJ's Money Laundering and Asset Recovery Section established a Digital Currency Initiative to expand and implement cryptocurrency-related training. According to the Report of the Attorney General's Cyber Digital Task Force in 2018, the Digital Currency Initiative encourages and enables more investigators, prosecutors, and department components to pursue virtual currency cases while developing and disseminating policy guidance on various aspects of cryptocurrency, including seizure and forfeiture.[114] Additionally, ICE-HSI's Cyber Crimes Center has collaborated with ICE-HSI's Illicit Finance and Proceeds of Crime Unit to develop cyber training focused on Dark Web investigations and illicit payment networks associated with fentanyl smuggling and distribution. According to ICE-HSI's Cyber Crimes Center officials, since 2018 at least 3,602 officials have been trained both domestically and internationally.

According to Treasury officials, in December 2019, Treasury's Office of Terrorism and Financial Intelligence hosted its inaugural Partnership to Combat Human Rights Abuse and Corruption event, bringing together over 100 nongovernmental organizations, industry, and government partners to combat human rights abuse and corruption through enhanced information sharing and coordination on illicit finance and corruption networks. These officials noted that in 2020, over 400 representatives attended the second annual event. Treasury officials told us it had led multiple panel discussions at these events on typologies of human trafficking including the use of virtual currencies, how financial tools can

[113]Deconfliction is the act of searching available data to determine if multiple law enforcement agencies are investigating the same target individual, organization, communications device, or other uniquely identifiable entity and, if so, of initiating coordination among the interested parties to prevent duplicative work or possible "blue on blue" situations (i.e., personnel from two or more law enforcement agencies unwittingly encountering each other during a law enforcement operation, such as an undercover situation).

[114]Department of Justice, Office of the Deputy Attorney General, *Report of the Attorney General's Cyber Digital Task Force.* (Washington, D.C.: July 2, 2018).

be used to support victims of human trafficking, and how to use technology to identify and combat human trafficking. FinCEN officials told us that FinCEN also regularly provides training to its law enforcement stakeholders in order to increase their efficiency and effectiveness in using BSA data to support virtual currency investigations. Further, in 2020 the Postal Inspection Service conducted a Basic Cryptocurrency and Dark Web 101 Training for Postal Inspection Service investigators designed to, among other things, introduce investigators to the Dark Web, provide functional knowledge of how virtual currency transactions are recorded on the blockchain, and how to identify tools and techniques used by criminals to protect their true identities. Finally, according to Treasury officials, Treasury's Office of Terrorist Financing and Financial Crimes, DOJ, and DHS in 2021 held a joint training for the casino industry on human trafficking, which highlighted the intersection between virtual currency and human trafficking.

Treasury Oversees Virtual Currency Money Services Businesses, but Lacks Information on Kiosk Locations

Treasury agencies are responsible for overseeing virtual currency MSBs, including virtual currency exchanges and kiosks. Registration requirements, examinations, and enforcement actions are methods used for oversight. Treasury agencies have also taken some steps to identify unregistered virtual currency MSBs. However, limited information on virtual currency kiosk location is collected, making it difficult to effectively identify and track virtual currency kiosk MSBs.

As discussed earlier, entities engaged in money transmission that conduct virtual currency transactions with U.S. customers, regardless of their location, must register as an MSB and comply with BSA/AML requirements. As of December 31, 2020, there were 354 active virtual currency MSBs registered with FinCEN. MSBs are required to maintain active registration by renewing every 2 years.

FinCEN has delegated authority to IRS to conduct BSA compliance examinations of virtual currency MSBs.[115] The number of BSA compliance examinations that IRS has completed has generally increased since it began conducting examinations in fiscal year 2015, from four in fiscal year 2015 to 21 in fiscal year 2020, totaling 66 BSA examinations completed from fiscal years 2015 to 2020.[116] FinCEN has also conducted 35 of its own targeted investigations of virtual currency MSBs from calendar year 2015 through 2020.

FinCEN has assessed over $180 million in civil money penalties for noncompliance to five virtual currency MSBs or individuals involved in MSB ownership since 2015. For example, in April 2019, FinCEN assessed a $35,350 civil money penalty against a peer-to-peer virtual currency exchanger for willfully violating the BSA registration, program, and reporting requirements. In addition to the fine, the peer-to-peer exchanger agreed to an industry bar prohibiting him from providing money transmission services.[117] In July 2017, FinCEN assessed a $110 million civil penalty against BTC-e, a foreign-located virtual currency exchange, for willfully violating U.S. anti-money laundering laws, and a $12 million penalty against the exchange's operator personally.[118] FinCEN also assessed a $60 million civil money penalty against the founder, administrator, and primary operator of Helix and Coin Ninja, virtual currency mixers, for violations of BSA in October 2020. According

[115]See 31 C.F.R. § 1010.810(b)(8), (c)(2), (g). FinCEN delegated certain authorities to IRS to enforce BSA provisions regarding records and reports of foreign financial agency transactions. 31 U.S.C. § 5314; 31 C.F.R § 1010.810(g). IRS also has been delegated authority to investigate criminal violations of the BSA. 31 C.F.R. § 1010.810(c)(2). IRS's Small Business/Self-Employed Division conducts BSA compliance examinations of nonbank financial institutions (such as money transmitters and casinos) and refers cases to FinCEN for potential civil enforcement action or to IRS-CI if the examiners believe a criminal violation may be involved. The Director of FinCEN maintains the overall authority for enforcement and compliance, including coordination and direction of procedures and activities of all other agencies delegated BSA authority. 31 C.F.R. § 1010.810(a).

[116]At the end of fiscal year 2020, IRS also had 38 ongoing examinations—with the most ongoing examinations, 55, in fiscal year 2019. IRS had 524 virtual currency entities in its examination database as of the end of fiscal year 2020. IRS officials told us that the increase in the number of virtual currency examinations was due to the expansion of the virtual currency industry and IRS providing specialized training to increase the number of examiners that can conduct virtual currency MSB examinations.

[117]FinCEN, *FinCEN Penalizes Peer-to-Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws* (Apr. 18, 2019).

[118]FinCEN, *FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales* (July 27, 2017).

to the FinCEN press release, the operator advertised its mixing services as a way for customers to anonymously pay for things like drugs, guns, and child pornography.[119]

IRS and FinCEN have also taken steps to identify unregistered virtual currency MSBs. For example, IRS officials told us that at the end of fiscal year 2020, they obtained contracts with three blockchain analytics vendors—one of which provided IRS with an inventory of virtual currency exchanges in December 2020. According to these officials, the inventory of exchanges provided by the blockchain analytics vendor has been the only reliable inventory of virtual currency exchanges that IRS has come across to date. IRS officials told us that they began an initiative in March 2021, utilizing the blockchain analytics tools they recently acquired, to identify unlicensed or noncompliant virtual currency entities, including peer-to-peer exchanges and decentralized exchangers. According to these officials, as of May 2021, this initiative was ongoing. FinCEN has also undertaken efforts to identify unregistered operators of virtual currency kiosks and estimates that, as of calendar year 2020, there were 133 unregistered kiosk operators in the United States. However, these estimates may be undercounts (see table 1).[120]

Table 1: Estimated Number of Operators of Virtual Currency Kiosks

Calendar Year	Number of Registered Kiosk Operators	Number of Known Unregistered Kiosk Operators	Estimated Number of Kiosk Operators in the U.S.
2018	87	104	191
2019	113	100	213
2020	164	133	297

Source: GAO analysis of FinCEN data | GAO-22-105462

Note: FinCEN officials told us they identified kiosks by researching open source information, such as articles, social media, and publicly available money services business registration data to identify registered and unregistered virtual currency kiosks. FinCEN officials stated that due to the nature of identifying unregistered entities, there are inherent limitations in knowing the full number of kiosk providers operating in the United States.

[119]FinCEN, *First Bitcoin "Mixer" Penalized by FinCEN for Violating Anti-Money Laundering Laws* (Oct. 19, 2020). FinCEN also assessed a $700,000 civil monetary penalty in May 2015 against Ripple Labs for willfully violating several BSA requirements by acting as an MSB and selling its virtual currency without registering with FinCEN, and by failing to implement and maintain an adequate AML program designed to protect its products from use by money launderers or terrorist financiers. See FinCEN, *FinCEN Fines Ripple Labs Inc., in First Civil Enforcement Action Against a Virtual Currency Exchanger* (May 5, 2015).

[120]FinCEN officials stated that due to the nature of identifying unregistered entities, there are inherent limitations in knowing the full number of kiosk providers operating in the U.S.

As shown in table 1, the number of kiosk operators has increased since 2018, and FBI officials told us that virtual currency kiosks are increasingly available. As market usage expands, FBI officials said they expect to see an increase in the use of virtual currency kiosks for illicit purposes, including for human and drug trafficking. International anti-money laundering standards issued by the Financial Action Task Force (FATF) state that supervisors should allocate and prioritize more supervisory resources to areas of higher anti-money laundering or terrorist financing risk—including within the virtual currency sector.[121] However, FinCEN does not routinely collect specific location information, such as physical addresses, on individual kiosks owned or managed by kiosk operators.

[121]On June 21, 2019, FATF adopted and issued an Interpretive Note to Recommendation 15 on New Technologies that clarifies international standards relating to virtual assets and includes that virtual asset service providers should be subject to risk-based supervision or monitoring. For the most recent standards, see Financial Action Task Force, *International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation*.

Traditional ATMs vs. Virtual Currency Kiosks: What's the Difference?

Traditional automated teller machines (ATMs) generally link an accountholder with that person's account at a regulated depository institution solely to verify balances and dispense currency. The accountholder's depository institution would be subject to Bank Secrecy Act (BSA) requirements that include verifying the identity of the customer. According to 2007 FinCEN guidance, traditional ATMs do not meet the definition of a money transmitter because the ATM is unable to transmit funds to third parties or to customer accounts at other financial institutions. Therefore, owner-operators of traditional ATMs are not subject to BSA requirements.

Virtual currency kiosks (commonly called "cryptocurrency ATMs" or "Bitcoin ATMs") are electronic terminals that enable the owner-operator to facilitate the exchange of virtual currency for cash or another type of virtual currency. These kiosks may connect directly to a separate virtual currency exchanger, which performs the actual transfer, or they may draw upon the virtual currency in the possession of the owner-operator of the electronic terminal.

According to FinCEN's 2019 guidance, an owner-operator of a virtual currency kiosk who uses an electronic terminal to accept currency from a customer and transmit the equivalent value in virtual currency (or vice versa) qualifies as a money transmitter both for transactions receiving and dispensing real currency or virtual currency. As a result, in accordance with BSA regulations for money transmitters, owner-operators of virtual currency kiosks are considered money transmitters and must comply with BSA regulations, such as verifying and collecting customer information on certain transactions, and maintaining an anti-money laundering program reasonably designed to prevent money laundering.

Source: GAO analysis of FinCEN guidance. | GAO-22-105462

Kiosk location data could be used to prioritize its supervisory resources on high-risk virtual currency kiosk locations.[122] Further, according to several law enforcement agencies we spoke with, kiosk location data, particularly when linked to operators of those locations, can improve information that law enforcement has available to identify the source of illicit transactions, such as human and drug trafficking. For example, an official from ICE-HSI told us that law enforcement agencies can figure out the location of the kiosk by searching different applications on the internet, but figuring out key information on the operators of kiosks is more challenging. Based on our review of a public website that provides data on virtual currency kiosks, operators can own over a thousand

[122]For example, high-risk geographic locations include those designated as a High Intensity Financial Crime Area or a High Intensity Drug Trafficking Area. These designations aim to concentrate law enforcement efforts at the federal, state, and local levels to combat money laundering and drug trafficking in designated high-intensity money laundering zones and in areas determined to be critical drug-trafficking regions of the U.S..

individual kiosks.[123] According to this website, the top three operators each had over 1,300 individual kiosk locations as of the end of January 2021. However, FinCEN records show that there were 164 registered kiosk operators at the end of calendar year 2020 and that they lack information on individual kiosk locations managed by these operators. This is because only the operator is required to register as an MSB, and FinCEN does not require the operator to report the specific locations, such as physical addresses, on individual kiosks they own or operate upon registration. As a result, it may be difficult to discern which kiosks belong to a registered MSB.

FinCEN's May 2019 guidance clarifies that BSA requirements apply to owners/operators of virtual currency kiosks and that they must comply with FinCEN regulations governing money transmitters, including registering with FinCEN and complying with BSA requirements such as verifying and collecting customer information on certain transactions.[124] FinCEN officials told us that BSA/AML regulations do not require virtual currency kiosk operators to submit individual kiosk locations when they register. However, the regulations require operators to provide the states where their branches are located and to separately identify the total number of kiosk locations they operate.[125] FinCEN officials also told us that FinCEN can request detailed kiosk location information when they examine the virtual currency entity and that requesting location information separately may cause undue burden on these entities. In addition, they told us that kiosk locations are constantly changing. However, FinCEN has not assessed the costs and benefits to impose a requirement for operators to report their kiosk locations, or how frequently kiosk location data should be provided.

[123]Coin ATM Radar, *Top 10 Bitcoin ATM Operators in the United States,* https://coinatmradar.com/charts/top-operators/united-states/, accessed January 26, 2021. This website provides kiosk locations and summary data on the number of kiosks under top operators by allowing operators of virtual currency kiosks to self-report kiosk locations so that users can locate their kiosks and utilize their services. Therefore, there is financial incentive for kiosk operators to accurately report and update the website.

[124]Financial Crimes Enforcement Network*, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*. See sidebar for differences in regulation between virtual currency kiosks and traditional ATMs.

[125]See Section IV (and its instructions) of the Registration of Money Services Business form (Item 34 and 35) and also the regulatory requirement to follow these instructions, in 31 C.F.R. § 1022.380(b)(1)(ii).

Section 6216 of the AML Act requires that the Secretary of the Treasury, consulting with other listed federal agencies, including IRS, undertake a formal review and make appropriate changes to improve the efficiency of BSA regulations and related guidance.[126] In addition, according to international anti-money laundering standards issued by FATF, to manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures.[127] Lastly, as discussed earlier, FATF recommendations require applying more supervisory resources to areas of higher anti-money laundering or terrorist financing risk, including within the virtual currency sector.[128]

Officials from several law enforcement components, blockchain analytics companies, and FinCEN told us that the degree to which virtual currency kiosks comply with BSA/AML regulations varies, with some kiosks implementing weak customer identification standards or not complying at all with BSA obligations. Kiosks with weak customer identification standards are susceptible to being used for illicit reasons and leave gaps in information collected on individual transactions as well as hindering law enforcement access to information to identify illicit transactions. By reviewing virtual currency kiosk registration requirements and taking appropriate actions, as needed, based on that review to collect more complete information from operators on individual kiosk locations, such as at MSB registration or renewal, FinCEN and IRS can better prioritize their supervisory resources on high-risk kiosk locations. Additionally, this information could help identify illicit kiosks and help law enforcement better target investigative resources.

[126]The formal review is to ensure that Treasury continues to appropriately safeguard the financial system from threats, including money laundering, among other threats to national security due to financial crime; to ensure such provisions require certain reports or records that are highly useful in countering financial crime; and to identify outdated, redundant, nonconforming, or non-risk-based regulations and guidance. Pub. L. No. 116-283, div. F, title LXII, § 6216, 134 Stat. at 4582-83.

[127]The Financial Action Task Force generally identifies a virtual asset service provider as a person or business that conducts operations for, or on behalf of, another person, including exchanging virtual currency to fiat currency or exchanging between one or more forms of virtual assets. For the most recent standards see Financial Action Task Force, *International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation*.

[128]Financial Action Task Force, *International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation*.

Selected Agencies Have Taken Steps to Address Some Challenges Related to the Global Nature of Virtual Currency and Human and Drug Trafficking Crimes

Criminals increasingly take advantage of the global nature of virtual currency to conduct their illicit activity. For example, criminals at times use virtual currency entities that are based in, or legally located in, a country that has little or no anti-money laundering compliance requirements to evade identification and detection by law enforcement. Treasury has taken steps to promote consistent application of anti-money laundering standards internationally by working through the U.S. delegation with international bodies, such as FATF. For example, in an effort led by the U.S., FATF updated its standards in June 2019 to require countries to implement effective registration, supervision, and other AML and countering the financing of terrorism requirements on virtual assets and virtual asset service providers.[129] In June 2019, FATF also issued guidance for a risk-based approach to virtual assets and virtual asset providers to further assist countries and virtual asset service providers in understanding and complying with anti-money laundering and countering the financing of terrorism obligations.[130] In July 2020 and July 2021, FATF completed 12-month reviews of the implementation of its revised standards and found that jurisdictions have made some progress, but several countries had not yet implemented the standards—meaning there is not yet a global regime to prevent the misuse of virtual currencies.[131] Treasury also led U.S. input to FATF's report on financial flows from human trafficking, which provides information on the risks, typologies, and red flag financial indicators of human trafficking. The report also provides best practices to address challenges in detecting, investigating, and prosecuting human trafficking, including the use of virtual currency in

[129]Financial Action Task Force, *Public Statement on Virtual Assets and Related Providers,* (Orlando, FL; June 21, 2019); and *Outcomes FATF Plenary, 16-21 June 2019* (Orlando, FL; June 21, 2019).

[130]Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Paris, France: June 2019). FATF has issued a draft proposal for public comment to update this guidance. See Financial Action Task Force, *Public Consultation on FATF Draft Guidance on a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Paris, France: March 2021).

[131]Financial Action Task Force,*12-Month Review Of The Revised FATF Standards On Virtual Assets And Virtual Asset Service Providers* (Paris, France: June 2020). Financial Action Task Force, *Second 12-Month Review of The Revised FATF Standards On Virtual Assets and Virtual Asset Service Providers* (Paris, France: July 2021).

human trafficking.[132] According to Treasury officials, this report has been used to encourage jurisdictions to investigate money laundering associated with human trafficking and work with the private sector and civil society to identify the activity.

There are also several provisions within the AML Act that encourage Treasury's coordination with international counterparts and facilitation of information sharing between financial institutions and their foreign branches, subsidiaries, and affiliates.[133] These efforts, if implemented, may help to address challenges related to the global nature of illicit activity using virtual currency by facilitating better global AML supervision. According to a FinCEN notice, it plans to propose amendments to BSA regulations regarding reports of foreign financial accounts to include virtual currency as a type of reportable account.[134] Officials told us that such regulatory change could assist in identifying foreign virtual currency exchanges, which may help law enforcement identify virtual currency in human and drug trafficking investigations. However, officials noted that making the regulatory amendment would require clearance through the agency and a formal notice and comment process—requiring agreement among various parties. In addition, FinCEN officials identified Section 9714 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal year 2021 as a provision that can help address money laundering concerns involving certain transmittals of funds connected with

[132]Financial Action Task Force*, Financial Flows from Human Trafficking* (Paris, France: July 2018).

[133]For example, Section 6108, Foreign Financial Intelligence Unit Liaisons; Section 6111 Increasing Technical Assistance for International Cooperation; Section 6112 International Coordination; Section 6212 Pilot Program on Information Sharing. Pub. L. No. 116-283, div. F, titles LXI, LXII, §§ 6108, 6111-12, 6212, 134 Stat. at 4559-60, 4563-64, 4576-79.

[134]Financial Crimes Enforcement Network, *Report of Foreign Bank and Financial Accounts (FBAR) Filing Requirement for Virtual Currency*, FinCEN Notice 2020-2. A report of foreign banks and financial accounts is a BSA requirement that certain U.S. taxpayers and residents are required to file with FinCEN annually if they have financial interest or signature or other authority over one or more foreign financial accounts with a total of more than $10,000, regardless of whether they reside within or outside the United States.

Russian illicit finance, which could include those involving foreign-based virtual currency entities.[135]

Federal prosecutors and law enforcement authorities have used Mutual Legal Assistance Treaties requests to obtain banking and other financial information and evidence from foreign countries for use in criminal investigations in the United States, including cases involving virtual currency. Officials from various law enforcement components, Treasury, and a blockchain analytics firm have identified some limitations in the Mutual Legal Assistance Treaties process, including that it can be a slow process, depending on the countries involved, and that it does not keep pace with criminals' instantaneous transactions and fast-changing digital evidence. Further, an official from Treasury stated that depending on the treaty status, some countries may not respond at all. Officials from law enforcement components also noted that some countries' privacy laws also make it challenging to obtain transaction data, including those involving virtual currency. However, according to some Treasury officials, provisions in the AML Act could expand agencies' access to international records, including cases involving virtual currency. For example, Section 6308 of the act states that DOJ and Treasury may subpoena foreign financial institutions that maintain U.S. correspondent accounts and request any records related to the correspondent account or any account

[135]Section 9714(a) allows Treasury to determine if financial institutions, classes of transactions, or types of accounts outside of the U.S. are considered of primary money laundering concern in connection with Russian illicit finance. Under paragraph (a)(2), it further provides Treasury the authority to require enhanced information collection concerning the transmittals of funds, or prohibit, or impose conditions upon the transmittals of funds (to be defined by the Secretary) by any domestic financial institution or agency, if the transmittal involves the institution, class of transaction, or type of account identified as of primary money laundering concern. Pub. L. No. 116-283, div. H, title XCVII, subtitle B, § 9714, 134 Stat. at 4838-39.

at the foreign bank, including records maintained outside of the United States.[136]

Law enforcement components also coordinate with international partners, such as Europol and the Five Eyes Law Enforcement Group, and have attachés stationed in different countries.[137] For example, the FBI has legal attaché offices covering more than 180 countries, territories, and islands around the world. The FBI legal attachés work with the law enforcement and security agencies in their host countries to coordinate investigations of interest to both countries. According to the 2018 DOJ Attorney General Cyber Digital Task Force Report, the FBI has supplemented 20 of these international offices with cyber-specific investigators to facilitate cooperation and information sharing to advance its cybercrime and national security investigations.[138] DHS officials stated that they have 78 attaché offices worldwide, which are important for international coordination. Officials from some law enforcement agencies told us that attachés are not a comprehensive solution to global coordination around the illicit use of virtual currency. However, others noted that attachés have been critical in facilitating international coordination by providing prompt and continuous exchange of information with foreign law enforcement agencies where attachés are located. The AML Act also formally establishes a Treasury Financial Attachés Program under which the Secretary of the Treasury is to appoint Treasury employees as a Treasury Financial Attaché.[139] In accordance with the act, attachés are responsible

[136]Pub. L. No. 116-283, div. F, title LXIII, § 6308, 134 Stat. at 4590-94. The statute is generally applicable to records that are the subject of any U.S. criminal investigation; any investigation of a violation regarding records and reports on monetary instruments transactions; a civil forfeiture action; or an investigation pursuant to section 5318A of title 31, U.S. Code. Correspondent relationships involve the provision of financial services by one financial institution, the correspondent institution, to another, the respondent institution. U.S. financial institutions that maintain correspondent relationships with a foreign financial institution that has failed to comply with a subpoena must end the relationship within 10 days of being notified of their customer's noncompliance. U.S. financial institutions that fail to comply may be fined up to $25,000 per day (up from $10,000 per day previously).

[137]Europol is the European Union's law enforcement agency. Europol supports the 27 European Union Member States in the fight against terrorism, cybercrime and other organized forms of crime. The Five Eyes Law Enforcement Group is an international coalition of law enforcement agencies from Australia, Canada, New Zealand, the United Kingdom, and the United States who share criminal intelligence and collaborate on operations to combat transnational crime.

[138]Department of Justice, Office of the Deputy Attorney General, *Report of the Attorney General's Cyber Digital Task Force.*

[139]Pub. L. No. 116-283, div. F, title LXI, § 6106, 134 Stat. at 4556-57.

for, among other things, establishing and maintaining relationships with foreign counterparts, conducting outreach to private sector entities, and coordinating with DOJ representatives who perform similar functions.

Emerging Technology Used to Facilitate Human and Drug Trafficking and Other Illicit Activity Presents New Challenges for Agencies

The increasing use of advanced obfuscation techniques makes blockchain analysis difficult and resource intensive for U.S. agencies. As discussed earlier, criminals are getting more sophisticated and using anonymity-enhanced tools or methods to obfuscate illicit transactions when facilitating criminal activities, including human and drug trafficking (see app. II). Effective tracing of illicit use of virtual currency is increasingly resource intensive and requires sophisticated computer software programs.

In response, agencies have developed in-house expertise and hired contractors among other practices, to trace illicit use of virtual currency. For example, ICE-HSI's Cyber Crimes Center developed in-house expertise and has hired three technical specialists—a Cyber Operations Officer, a Cyber Security Specialist, and a Forensic Analyst—to address an increasing need for advanced training and skills associated with countering the use of virtual currency for illicit activities. Additionally, in 2017, the Money Laundering and Asset Recovery Section hired a dedicated Digital Currency Counsel as a subject matter expert to provide virtual currency expertise to prosecutors, investigators, and policy makers within DOJ.[140] IRS-CI officials told us that when it comes to virtual currency investigations, officials prefer to develop their own internal skill capabilities, with about 80 percent or more of their expertise in-house, because of the large percentage of their cases that involve virtual currency. In addition to developing in-house expertise, nearly all of the law enforcement and financial regulatory components we spoke with told us that they also effectively partner with third parties, including blockchain analytics companies and academic institutions with specialized research

[140]In July 2021, FinCEN announced it had established and filled its first-ever Chief Digital Currency Advisor position. According to the press release, the Chief Digital Currency Advisor is to advance FinCEN's leadership role in the digital currency space by working across internal and external partners toward strategic and innovative solutions to prevent and mitigate illicit financial practices and exploitation.

capabilities, as necessary, to support virtual currency investigations or examinations.

Emerging technologies such as a decentralized exchange, where users may convert virtual currencies for other types of virtual currency, or convert the funds into fiat currency, may pose challenges to law enforcement and regulators. According to FinCEN officials, these decentralized exchanges can pose challenges to the current regulatory regime, as the regime relies on regulating financial intermediaries as the primary mechanism for overseeing financial transactions. Decentralized exchanges are software programs that operate on a peer-to-peer network of computers running a blockchain platform designed such that they may not be controlled by a single person or group of persons (that is, they do not have an identifiable administrator). FinCEN officials told us that without an identifiable administrator or a financial intermediary employed, it is difficult to impose BSA/AML regulations. FinCEN has taken some steps to address this emerging technology. For example, FinCEN guidance clarifies that BSA requirements apply to persons using decentralized finance exchanges to operate as money transmitters. [141]

FinCEN officials told us that while regulations in place address some decentralized exchanges models, implementing regulations is challenging because decentralized exchanges may not have an identifiable administrator or operator to contact in order to implement compliance. Officials also told us that they are considering what regulatory and statutory changes are necessary to keep BSA requirements sufficiently tailored to current technology. FinCEN officials added that the AML Act includes provisions to help address emerging technology challenges. For example, the AML Act requires Treasury to periodically convene a global anti-money laundering and financial crime symposium focused on how new technology can be used to more effectively combat financial crimes and other illicit activities.[142] FinCEN has begun to address requirements in

[141]Department of the Treasury, Financial Crimes Enforcement Network, *FinCEN Guidance - Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*.

[142]Pub. L. No. 116-283, div. F, title LXII, § 6211, 134 Stat. at 4575-76. Section 6211 of the AML Act requires the Department of the Treasury to periodically convene a global anti-money laundering and financial crime symposium focused on how new technology can be used to more effectively combat financial crimes and other illicit activities. The AML Act further requires that such symposiums shall be convened in coordination with a new Bank Secrecy Act Advisory Group Subcommittee on Innovation and Technology, as established under Section 6207 of the AML Act.

the AML Act. In a February 2021 statement, FinCEN noted that the Financial Crimes Tech Symposium would build upon FinCEN's ongoing Innovation Initiative, including its Innovation Hours Program, which began in March 2019.[143] In a recent report on the Innovation Hours Program, FinCEN highlighted how, as a result of an Innovation Hours Program event in December 2020, FinCEN learned about a series of new innovative solutions developed through tech sprints (also known as "hackathons") to find perpetrators of child sexual abuse materials and to track the perpetrators' use of virtual currency.[144]

Conclusions

Treasury agencies, such as FinCEN and the IRS, have taken steps to identify unregistered virtual currency MSBs. However, they face challenges in identifying and tracking virtual currency kiosk locations, including physical addresses. FinCEN has regulations in place for virtual currency kiosks to register as an MSB, but these regulations apply to the operator rather than to the individual kiosk location. The registration requirements do not require kiosk operators to report the physical addresses of individual locations of the kiosks they operate or own. As we have noted, kiosk operators can own over 1,000 kiosks. Therefore, this leaves a gap in the information that FinCEN and law enforcement have on virtual currency kiosk locations and their operators. Indeed, several law enforcement agencies we spoke with reported that kiosk location data, particularly when linked to operators of those locations, can improve the information that law enforcement has available to identify the source of illicit transactions, such as human and drug trafficking. By reviewing virtual kiosk registration requirements and taking appropriate actions, as needed, based on that review, to collect more complete information on individual kiosk locations, such as at registration or renewal, FinCEN and IRS can better prioritize their supervisory resources on high-risk kiosk locations. Additionally, this information could help identify illicit kiosks and help law enforcement better target investigative resources.

[143]FinCEN Statement on Financial Crimes Tech Symposium (Feb. 4, 2021). https://www.fincen.gov/news/news-releases/fincen-statement-financial-crimes-tech-symposium, accessed March 29, 2021.

[144]Financial Crimes Enforcement Network, *Innovation Hours Program Emerging Themes and Future Role in AML Act Implementation (May 2019 - February 2021) (*March 2021).

Recommendations for Executive Action

We are making two recommendations, including one to the IRS and one to FinCEN.[145] Specifically:

The Commissioner of IRS should review the MSB registration requirements for virtual currency exchanges and administrators that operate virtual currency kiosks and make recommendations to the Director of FinCEN, based on that review, such as recommendations on requiring kiosk operators to submit the locations, including physical addresses of kiosks they own or operate, upon MSB registration, and update this information upon reregistration or other appropriate interval. (Recommendation 1)

The Director of FinCEN, in consultation with the Commissioner of IRS, should review MSB registration requirements for virtual currency exchanges and administrators that operate virtual currency kiosks and take appropriate actions, as needed, based on that review, such as requiring kiosk operators to submit the locations, including physical addresses of kiosks they own or operate, upon MSB registration, and update this information upon reregistration or other appropriate interval. (Recommendation 2)

Agency Comments

We provided a draft of this report to DHS, DOJ, the Department of Labor, the Department of State, IRS, Office of National Drug Control Policy, Treasury, and the Postal Inspection Service for review and comment. Treasury concurred with the recommendation directed at FinCEN in an email from its audit liaison and provided technical comments, which we incorporated as appropriate. IRS's audit liaison concurred with the recommendation directed at the agency through oral comments. The Department of State and DHS provided technical comments, which we incorporated as appropriate, but provided no additional comments. Further, audit liaisons for DOJ and the Department of Labor reported

[145]In the sensitive version of this report, GAO-21-104129SU, we made nine additional recommendations, including that FinCEN, ICE-HSI, Secret Service, DEA, FBI, DOJ's Criminal Division, DOJ's Justice Management Division, IRS Criminal Investigations, and the Postal Inspection Service, to the extent practicable, identify and employ improved methods to consistently capture data on the use of virtual currency in human and drug trafficking.

having no comments by email. The Office of National Drug Control Policy and the Postal Inspection Service did not comment on this report.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the appropriate congressional committees. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact Gretta L. Goodwin at (202) 512-8777 or goodwing@gao.gov or John H. Pendleton at (202)-512-8678 or pendletonj@gao.gov. GAO staff who made key contributions to this report are listed in appendix IV.

Gretta L. Goodwin, Director, Homeland Security and Justice

John H. Pendleton, Director, Financial Markets and Community Investment

Appendix I: Objectives, Scope, and Methodology

Various agency components within the Department of the Treasury (Treasury), the Department of Homeland Security (DHS), and the Department of Justice (DOJ) are responsible for enforcing U.S. laws and regulations related to the use of virtual currencies. You asked us to review the flow of money from virtual currencies and online marketplaces to buy, sell, or facilitate the financing of goods or services associated with sex trafficking and drug trafficking. This report examines (1) what is known about the use of virtual currency for human and drug trafficking and to what extent do U.S. agencies collect data on these topics; and (2) the extent to which U.S. agencies have taken steps to counter human and drug trafficking facilitated by the use of virtual currency, and what challenges, if any, these agencies face.

Identifying Federal Agencies with Expertise In Virtual Currency, Human Trafficking and Drug Trafficking

To inform both objectives, we first sought to identify which federal agencies had extensive or specific experience or expertise with virtual currency as it relates to human and drug trafficking. To do this, we developed a list of federal components involved in countering virtual currency use for human and drug trafficking by (1) holding meetings with DOJ, DHS, Treasury, the U.S. Postal Service (USPS), the Office of National Drug Control Policy, the Department of State, and the Department of Labor; (2) obtaining information from each of these agencies on relevant agency components (e.g., subagencies, divisions, units) as well as partnerships with other federal components; and (3) reviewing these agencies' websites for organizational charts and descriptions of agency components.[1] On the basis of these sources, we compiled a list of 60 federal components. We further developed a questionnaire to help us better understand each component's level of

[1]Throughout this report, we refer to components of federal agencies (e.g., subagencies, divisions, units). When we refer to the department level (e.g., DOJ, DHS, Treasury, USPS), we use the term agencies.

involvement in virtual currency, and combatting human trafficking and drug trafficking. The questionnaire included 12 open-ended and close-ended questions, such as questions about the components' level of involvement in the past 3 years in investigations and prosecutions in the areas of virtual currency, human trafficking, and drug trafficking, among other questions.[2] The questionnaire was distributed to 58 of 60 federal components by email, requesting that each component complete the questionnaire separately.[3] We received completed questionnaires from 56 of the 58 components that were distributed the questionnaire.[4] Information collected through the interviews and questionnaire responses cannot be generalized to all federal components but provides useful information to address both of our objectives.

We obtained and systematically assessed components' responses to our questionnaire by first reviewing the entirety of the returned questionnaire for each component and determining whether the component was "in" or "out" of scope, based on whether a component had demonstrated experience or expertise with virtual currency and a nexus to at least one of the crime types of focus for this review (i.e., labor, sex, and drug trafficking; money laundering related to those crimes). We then coded each component into a level of priority (Tier 0=least relevant components/out of scope, Tier 1=most relevant components, Tier 2=less relevant components). In cases where the analyst could not make a clear determination, a second analyst and the original analyst discussed the information provided and made a final determination. A second analyst reviewed all determinations (including "in" or "out" of scope and tier determinations). Tier 1 determinations were made on the basis of whether a component had demonstrated extensive and specific experience or expertise with virtual currency and a nexus to one of the crime types (i.e., labor, sex, and drug trafficking; money laundering related to those crimes). Tier 2 determinations were made when a component's response

[2]The questionnaire was peer reviewed by our in-house methodologists.

[3]We separately reached out to the two agencies that we did not send questionnaires to in order to conduct more targeted follow-up based on their roles.

[4]We followed up with components that did not initially provide questionnaire responses and received responses to all but two questionnaires. We also followed up with components, as needed, to clarify and make sure we had complete responses. In the two cases where we did not receive a completed questionnaire, we found that information provided in interviews and email responses sufficiently captured the level of information needed to understand each component's level of involvement in virtual currency, and in combatting human trafficking, and drug trafficking.

indicated that their involvement with virtual currency and a nexus to one of the crime types was incidental or a nonspecific experience. Through this analysis, we identified 14 components (13 Tier 1 and one Tier 2) that had the most experience and/or expertise countering human and/or drug trafficking facilitated by the use of virtual currency and covered a variety of expertise, including relevant law enforcement agencies and federal regulatory agencies (see table 2).[5] Components selected included investigative, policy, prosecutorial, enforcement, and technical specialists.

Table 2: Selected Federal Components

Department of Homeland Security: Immigration and Customs Enforcement Homeland Security Investigations
Cyber Crimes Center
Illicit Finance Proceeds of Crimes Unit
Department of Justice (DOJ): Criminal Division
Computer Crime and Intellectual Property Section
Money Laundering and Asset Recovery Section
DOJ: Drug Enforcement Administration
Cyber Support Section
DOJ: Federal Bureau of Investigation
Criminal Investigative Division
Joint Criminal Opioid Darknet Enforcement team
National Cyber Investigative Joint Task Force
Department of the Treasury (Treasury): Office of Terrorism and Financial Intelligence (TFI)
Office of Terrorist Financing and Financial Crimes
Treasury: Financial Crimes Enforcement Network
Enforcement and Compliance Division
Intelligence Division

[5]Our selection included 13 Tier 1 components and one Tier 2 component (i.e., the National Cyber Investigative Joint Task Force). We interviewed the National Cyber Investigative Joint Task Force, a Tier 2 component, because several Tier 1 components mentioned their role in countering human and drug trafficking that involves virtual currency. We also conducted a targeted interview with the Secret Service (another Tier 2 component) to understand their role and practices in countering human and drug trafficking that involves virtual currency, and reviewed their documentation, such as training materials. As part of this interview and review of information provided by the Secret Service, we identified that the Secret Service had expertise in virtual currency, contributes as a member of the National Cyber Investigative Joint Task Force, and is a partner with the National Center for Missing and Exploited Children. We did not hold a semistructured interview with the Secret Service because they initially told us their primary focus is on financial crimes and not human and drug trafficking crimes.

Policy Division
Treasury: Internal Revenue Service
Criminal Investigations Division
United States Postal Service: U.S. Postal Inspection Service
Cyber Analytics Program

Source: GAO analysis. | GAO-22-105462

Note: We also conducted a targeted interview with DHS's Secret Service to understand their role and practices in countering human and drug trafficking that involves virtual currency and reviewed their documentation, such as training materials. We did not hold a semistructured interview with the Secret Service because they initially told us their primary focus is on financial crimes and not human and drug trafficking crimes.

For the 14 government components we identified as having the most experience and/or expertise countering human and/or drug trafficking facilitated by the use of virtual currency, we performed semistructured interviews.[6] We met with most components in separate interviews, except for two components within the Financial Crimes Enforcement Network (FinCEN).[7] We developed a standard set of open-ended questions focused on what is known about virtual currency use in illicit activity, such as human and drug trafficking, and federal efforts to counter human and drug trafficking facilitated by virtual currency. We also asked agency officials to identify key human and drug trafficking legal cases in which virtual currency was used to facilitate these illicit activities.

Consideration of Third Party Views

To inform both objectives, we selected and interviewed a nongeneralizable sample of five third-party organizations actively involved in analyzing virtual currency transactions or combatting human trafficking. We identified these third parties by asking agency officials and reviewing our relevant prior reports. We selected two blockchain analytic firms that focus on virtual currency and three nonprofits focused on combatting

[6]A semistructured interview methodology generally involves asking a similar subset of questions of multiple interviewees.

[7]We interviewed FinCEN's Intelligence Division and Policy Division together because of the interactive nature of their work. We interviewed FinCEN's Enforcement and Compliance Division separately because of their focus on examinations and enforcement.

human trafficking.[8] Through structured interviews, we obtained their perspectives on (1) notable trends in the virtual currency market, (2) methods used by criminals to facilitate human and drug trafficking using virtual currency, and (3) any challenges associated with countering human and drug trafficking transactions that involve the use of virtual currency. We did not identify a third-party entity that could speak to the nexus between virtual currency and drug trafficking because agency officials and other knowledgeable individuals did not suggest a third party within the scope of our review. For context, we also reviewed studies from blockchain analytic firms and nonprofits focused on human trafficking issues.[9]

Review of Applicable Laws, Regulations, Guidance, and Court Cases

To inform both objectives, we reviewed applicable federal laws, regulations, and guidance. For example, we reviewed applicable Bank Secrecy Act/Anti-money Laundering (BSA/AML) regulations; FinCEN guidance; the Anti-Money Laundering Act of 2020, enacted in January 2021 (AML Act); and other relevant laws such as human and drug trafficking statutes, among others.[10] In addition, we reviewed relevant international anti-money laundering standards and guidance issued by the intergovernmental Financial Action Task Force (FATF). Further, we identified and reviewed agency documents such as the Attorney General's Cyber Digital Task Force *Cryptocurrency Enforcement*

[8]The two blockchain analytics firms interviewed included Chainalysis and CipherTrace. The three human trafficking nonprofit organizations we identified included the Human Trafficking Institute, the Human Trafficking Legal Center, and Polaris. The Human Trafficking Institute and the Human Trafficking Legal Center conduct human trafficking research. Polaris works to prevent and reduce sex and labor trafficking in the U. S. and Mexico and, since 2007, has operated the National Human Trafficking Hotline.

[9]For example, *see* Chainalysis, *The 2020 State of Crypto Crime* (January 2020); CipherTrace, *Cryptocurrency Crime and Anti-Money Laundering Report* (February 2021); and Polaris, *Using an Anti-Money Laundering Framework to Address Sex Trafficking Facilitated by Commercial Sex Advertisement Websites* (July 2020).

[10]Currency and Foreign Transactions Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified, as amended, primarily at 31 U.S.C. §§ 5311, *et seq.*, among other places in the U.S. Code) (commonly referred to as the "Bank Secrecy Act" or "BSA"). The AML Act was enacted as Division F of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, div. F, 134 Stat. 3388, 4547-4633.

Framework; DEA's National Drug Threat Assessment; and Treasury's National Strategy on Illicit Finance; as well as DHS and DOJ press releases publicly accessible on their websites.[11]

We identified and analyzed six criminal cases to illustrate how virtual currency could facilitate illicit activity in human and drug trafficking. We identified 33 cases by reviewing DHS and DOJ press releases as well as case documentation identified on legal online databases. We compiled a list of cases; provided it to selected federal components; and, during interviews with federal components, we requested agency officials' perspectives on relevant cases that involved virtual currency as well as human or drug trafficking. From there, we selected six notable or recent cases. We used these cases to illustrate examples of different ways that virtual currency was allegedly used to facilitate human and drug trafficking, as well as the various statutes federal prosecutors use to charge related criminal conduct.

Objective 1: Use of Virtual Currency for Human and Drug Trafficking and Federal Data Collection Efforts

To address the first objective to examine what is known about the use of virtual currency for human and drug trafficking, we conducted semistructured interviews with officials from the 14 selected components (selection process described above) for their perspectives on (1) the nexus between virtual currency and illicit activity, such as human and drug trafficking, as well as (2) trends in the virtual currency market, including virtual currency tools and online venues, and the extent virtual currency is used to carry out illicit activities, such as human and drug trafficking.[12] We documented agency officials' responses to our questions

[11]For example, *see* Department of Treasury, *2020 National Strategy for Combating Terrorist and Other Illicit Financing* (February 6, 2020); Department of Justice, Office of the Deputy Attorney General, Cyber Digital Task Force, *Cryptocurrency Enforcement Framework* (Washington, D.C.: October 2020).

[12]We also conducted a targeted interview with officials from the Secret Service to understand their role and practices in countering human and drug trafficking that involves virtual currency and reviewed their documentation, such as training materials. We did not hold a semistructured interview with officials from the Secret Service because they initially told us their primary focus is on financial crimes and not human and drug trafficking crimes.

and analyzed responses to establish prevalence of themes, such as virtual currency's use on platforms in the online commercial sex market, for the sale and purchase of illegal drugs on Dark Web marketplaces, and the extent virtual currency is used to facilitate human and drug trafficking. We further reviewed documentation provided or identified by these components, such as agency policies and reports or information from sources knowledgeable officials at these components identified as informative or authoritative. In addition, we considered the results of our prior work.[13]

Objective 2: Steps Taken and Challenges Faced By Federal Agencies to Counter Human and Drug Trafficking Facilitated By Virtual Currency

To address the second objective, to examine the extent to which U.S. agencies have taken steps to counter human and drug trafficking facilitated by the use of virtual currency, we conducted semistructured interviews with the 14 selected components (selection process described above) for their perspectives on (1) laws, regulations, and guidance used to counter human and drug trafficking facilitated by virtual currency; (2) practices used to identify, investigate, and prosecute individuals who use virtual currency to facilitate human and drug trafficking—such as utilizing BSA data and coordination with other federal agencies; and (3) technologies used to counter the use virtual currency to facilitate human and drug trafficking—such as in-house expertise and blockchain analytics

[13]For example, see GAO, *Sex Trafficking: Online Platforms and Federal Prosecutions*, GAO-21-385 (Washington, D.C.: June 2021); *Virtual Currencies: Additional Information Reporting and Clarified Guidance Could Improve Tax Compliance* GAO-20-188 (Washington, D.C.: Feb 12, 2020); and *Virtual Currencies: Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges*, GAO-14-496 (Washington, D.C.: May 29, 2014).

tools.[14] We also asked questions about challenges related to these three topics. For example, we asked selected components if the current legal or regulatory structure poses any challenges; if virtual currency poses any unique technological challenges; and if the global nature of virtual currencies pose any challenges to investigating human and drug trafficking cases that involve virtual currency. We aggregated responses from our semistructured interviews to identify themes and trends in these areas.

We also reviewed guidance associated with laws and regulations and documentary evidence of U.S. agencies' efforts to counter human and drug trafficking that involve virtual currency. For example, we identified and reviewed existing FinCEN guidance and advisories that address human and drug trafficking.[15] We also reviewed FinCEN's guidance and advisories that clarify BSA/AML obligations for virtual currency entities and assist financial institutions in identifying and reporting suspicious activity related to criminal exploitation of virtual currency for illicit financing purposes, such as human and drug trafficking.[16] Further, we identified FinCEN's notice of proposed rulemakings that would impose greater customer identification and verification requirements at lower thresholds

[14]We also conducted a targeted interview with the Secret Service to understand their role and practices in countering human and drug trafficking that involves virtual currency and reviewed their documentation, such as training materials. As part of this interview and review of information provided by the Secret Service, we identified that the Secret Service had expertise in virtual currency, contributes as a member of the National Cyber Investigative Joint Task Force, and is a partner with the National Center for Missing and Exploited Children. We did not hold a semistructured interview with the Secret Service because they initially told us their primary focus is on financial crimes and not human and drug trafficking crimes.

[15]For example, *see* Financial Crimes Enforcement Network, *Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity*, FIN-2020-A008 (Oct. 15, 2020) and *Advisory to Financial Institutions on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids*, FIN-2019-A006 (Aug. 21, 2019).

[16]*For example, see* Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001 (May 9, 2019) and *Advisory on Illicit Activity Involving Convertible Virtual Currency*, FIN-2019-A003 (May 9, 2019).

and increased reporting of certain virtual currency transactions.[17] In addition, we reviewed information that agencies provided on partnerships with other federal agencies and third parties, as well as training materials used by agencies to educate agents about virtual currency use in illicit activity.

To examine Treasury's efforts to oversee virtual currency money services businesses (MSB), we identified and reviewed registration requirements and MSB e-filing instructions, examination practices, and enforcement actions.[18] We interviewed officials from FinCEN's Enforcement and Compliance Division and IRS's Small Business/Self-Employed Division on their virtual currency MSB examination practices, investigations, and coordination on examinations of virtual currency MSBs. We also obtained their perspectives on the utility of these efforts as well as any challenges they face. We analyzed FinCEN's enforcement actions by reviewing their website for actions against virtual currency MSBs from calendar year 2015 through 2020, and reviewing related press releases and assessments of civil money penalties to identify the number of enforcement actions and value of assessments against these virtual currency MSBs.

To examine Treasury's efforts to oversee virtual currency kiosks—a specific type of virtual currency MSB—we reviewed FinCEN data on registered and unregistered operators of virtual currency kiosks. We assessed these data by discussing the data with agency officials and comparing data on kiosk operators with a public website described below. We found these data to be sufficiently reliable for the purposes of providing the number of registered kiosk operators and FinCEN's estimates for the number of unregistered kiosk operators that they have

[17]*See* Threshold for the Requirement To Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds That Begin or End Outside the United States, and Clarification of the Requirement To Collect, Retain, and Transmit Information on Transactions Involving Convertible Virtual Currencies and Digital Assets With Legal Tender Status, 85 Fed. Reg. 68,005 (Oct. 27, 2020) (to be codified at 31 C.F.R. pts. 1010, 1020), and *Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets,* 85 Fed. Reg. 83,840 (Dec. 23, 2020) (to be codified at 31 C.F.R. pts. 1010, 1020, 1022).

[18]For registration requirements, we reviewed prior GAO reports, MSB regulations, and filing instructions described in Financial Crimes Enforcement Network, *Registration of Money Services Business (RMSB) Electronic Filing Instructions,* version 1.0 (July 2014).

identified.[19] We reviewed a public website that provides data on virtual currency kiosks and the number of kiosks under the top operators, operating the largest number of kiosks.[20] We assessed the reliability of information posted on this website by discussing it with agency officials and comparing information on the top 10 kiosk operators identified on the website with information available to law enforcement. We found information posted on this website sufficiently reliable for estimating the number of kiosks for large operators.[21] We asked law enforcement—including DOJ, DHS, IRS-CI, and the Postal Inspection Service—their perspectives on challenges that virtual currency kiosks pose in countering the illicit use of virtual currency. We compared Treasury's oversight of virtual currency kiosks with criteria in the AML Act and international anti-money laundering standards.[22]

We conducted this performance audit from February 2020 to September 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We subsequently worked with DOJ, from October 2021 to December 2021 to prepare this version of the original sensitive report for public release. This public version was also prepared in accordance with these standards.

[19]FinCEN officials identified kiosks by researching open source information, such as articles and social media, and publicly available money services business registration data to identify registered and unregistered virtual currency kiosk. FinCEN officials stated that due to the nature of identifying unregistered entities, there are inherent limitations in knowing the full number of kiosk providers operating in the United States.

[20]https://coinatmradar.com/charts/top-operators/united-states/.

[21]Further, since the website allows operators of virtual currency kiosks to self-report kiosk locations so that users can locate virtual currency kiosks and utilize their services, there is financial incentive for kiosk operators to accurately report and update the website.

[22]See Pub. L. No. 116-283, div. F, title LXII, § 6216, 134 Stat. at 4582-83 and Financial Action Task Force, *International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation, The FATF Recommendations* (Paris, France: October 2020).

Appendix II: Virtual Currency Tools and Online Venues That Criminals have Used to Obfuscate and Facilitate Illicit Activities

Criminals have used various virtual currency tools and online venues to avoid detection in carrying out crimes facilitated by virtual currency, such as human and drug trafficking. Virtual currency tools in use today consist of mixing virtual currencies from different individuals to make the source and use of the currency difficult to trace and converting virtual currency to another virtual currency by moving the currency from one blockchain to another in rapid sequence, among other methods. Further, online venues, such as the Surface Web, the Dark Web, and Dark Web marketplaces are used to facilitate illicit activities with virtual currency.

Anonymity-enhanced Virtual Currency Tools

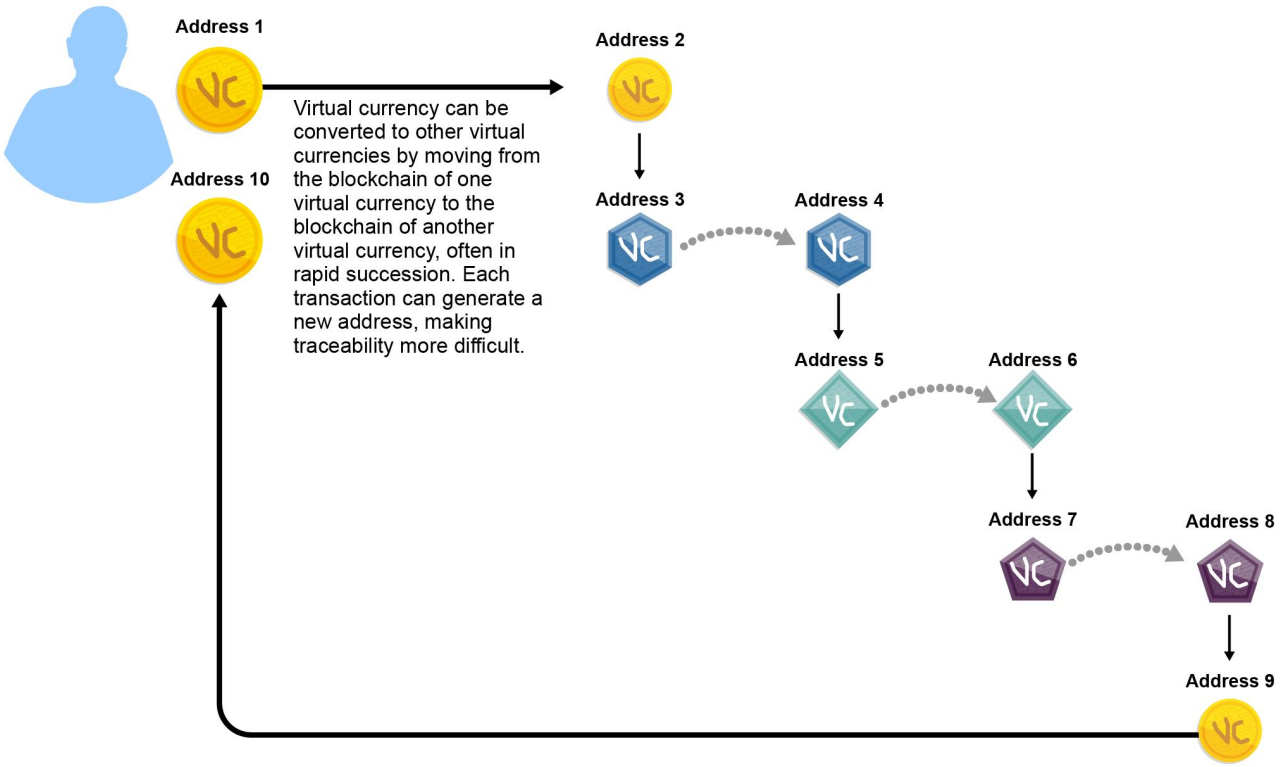
Privacy coins and transactional methods, such as chain hopping, mixers or tumblers, and peel chains, are technological tools or methods that may be used to conceal criminal activity, such as human and drug trafficking. They can also make illicit transactions harder to trace. Criminals may also use a combination of these tools, further complicating the tracing of virtual currency transactions to illicit activities, according to officials from the Immigration and Customs Enforcement – Homeland Security Investigations' (ICE-HSI) Illicit Finance Proceeds of Crimes Unit. Officials from the Department of Justice's (DOJ) Computer Crime and Intellectual Property Section stated that traffickers' use of multiple obfuscation methods is the greatest challenge their component faces when countering illicit transactions that use virtual currency for facilitating human and drug trafficking.

- **Privacy coins** use nonpublic or private blockchains and have technical encryption features (e.g., built-in "mixing" capability, described below) that make it more difficult to trace or to attribute transactions. These virtual currencies are often exchanged for other

virtual currencies, such as Bitcoin, in a technique commonly referred to as “chain hopping,” as described below. Financial Crimes Enforcement Network (FinCEN) officials stated that while privacy coins make up a small portion of the virtual currency market, they have seen an increase in the use of these virtual currencies to facilitate illicit activities, including on Dark Web marketplaces.

- **Chain hopping** involves transferring one virtual currency to another virtual currency on a different blockchain, often in rapid succession. Criminals can individually attempt to conceal their virtual currency transactions by shifting the trail from the blockchain of one virtual currency to the blockchain of another virtual currency. For example, if an individual has a Bitcoin wallet, which is where the blockchain is published, but then sets up a wallet for a different type of virtual currency, such as Monero, on a different blockchain, the individual could move Bitcoins to the Monero wallet, ultimately “jumping” from different blockchains, according to officials from ICE-HSI’s Cyber Crimes Center. Chain hopping can also be done through a virtual currency exchange or private company that offers this service for a fee. Figure 4 depicts an example of how chain hopping works.

Figure 4: Example of How Virtual Currency Transactions Can Be Moved Through "Chain Hopping"



Source: GAO analysis of Attorney General's Cyber Digital Task Force, Cryptocurrency Enforcement Framework. | GAO-22-105462

- **Mixers** or **tumblers** are centralized private services that mix the virtual currency of several users during transfers to increase anonymity.[1] For a fee, a customer can send virtual currency to a specific address controlled by the mixer. The mixer then commingles this virtual currency with funds received from other customers before sending it to the requested recipient address.[2] Some privacy coins have a built-in mixing capability. ICE-HSI's Cyber Crimes Center

[1]Mixers or tumblers are money transmitters and subject to Bank Secrecy Act (BSA) requirements under FinCEN regulations. Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual currencies*, FIN-2019-G001 (May 9, 2019).

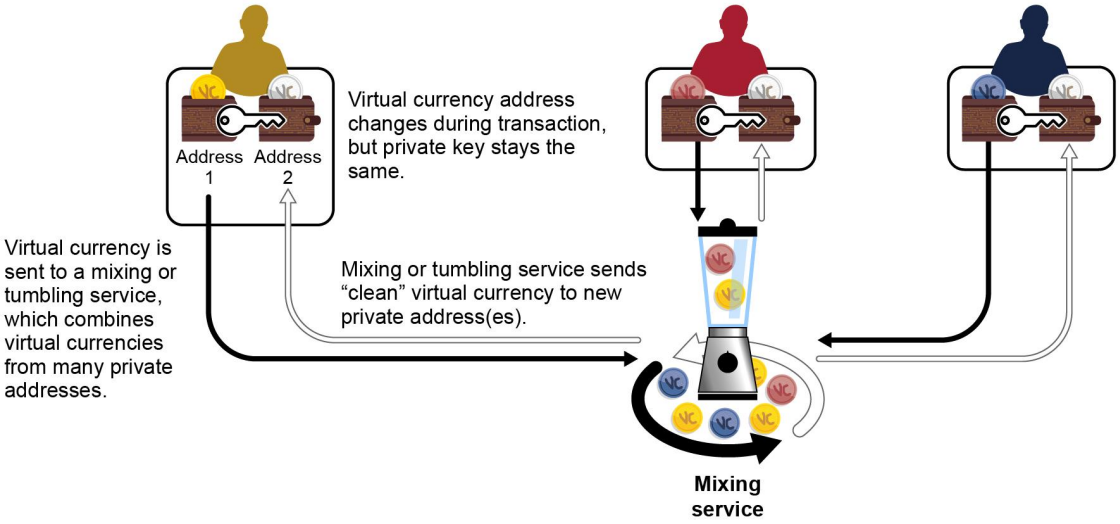
[2]In February 2020, law enforcement officials shut down Helix, a Dark Web virtual currency service that functioned as a mixer, allowing customers to send Bitcoin to designated recipients that concealed the Bitcoin's source or owner. Helix also provided money-laundering services to AlphaBay customers, a well-known Dark Web marketplace for facilitating drug trafficking, among other illicit activities, that is described in more detail below. Helix laundered over 350,000 bitcoins ($300 million worth), including proceeds of illegal drug sales, along with other criminal transactions.

officials stated that the use of mixers or tumblers may decrease in time because of the expense. As more virtual currency is moved, high transaction fees in some virtual currencies make the mixing or tumbling service more expensive to use, according to ICE-HSI's Cyber Crimes Center officials. Further, criminals can use other obfuscation services, such as chain hopping, that are less expensive.

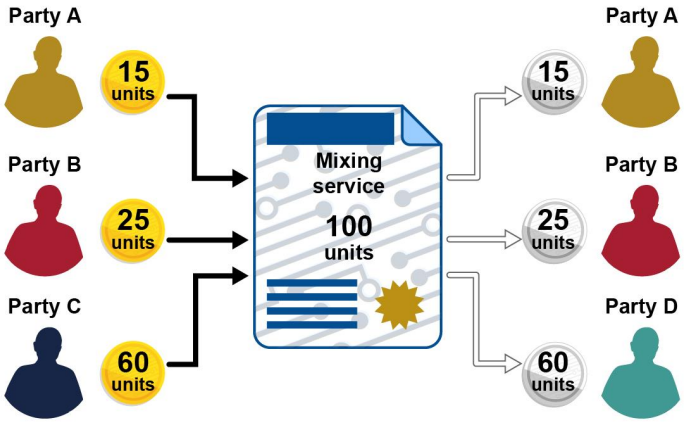
While mixers or tumblers may operate as private companies offering services to commingle funds, some mixing protocols may be used in a more decentralized manner that involves multiple virtual currency users coordinating to create a single transaction, making traceability more difficult. According to a FinCEN official, while mixers or tumblers can be flagged and pursued legally, decentralized mixing transactions may be more difficult to target. Figure 5 depicts examples of how centralized and decentralized mixers or tumblers can work.

Figure 5: Example of How Virtual Currency Transactions Can Be Moved Through Centralized and Decentralized "Mixers" or "Tumblers"

Centralized mixers or tumblers



Decentralized mixer

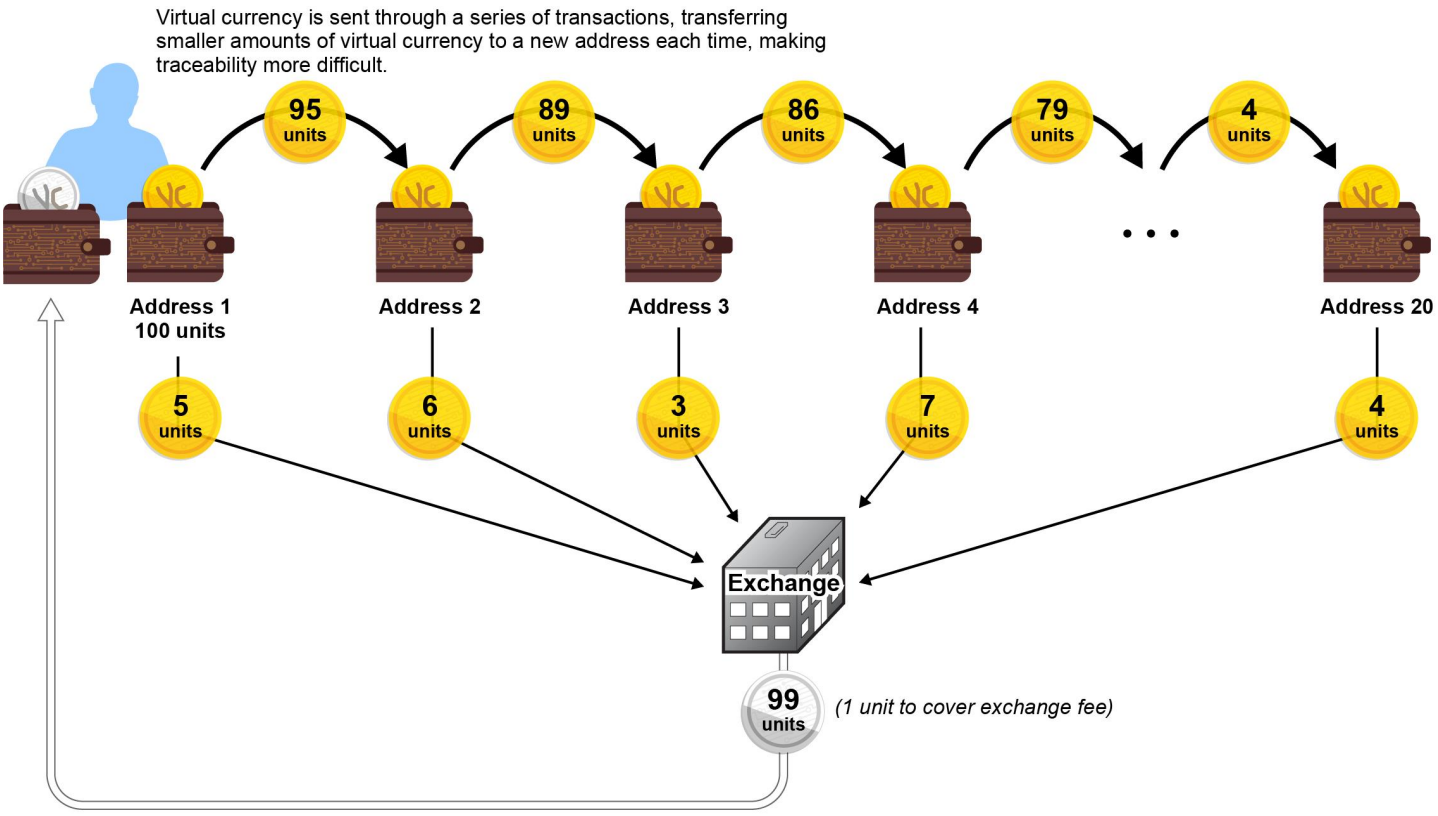


Through a private, decentralized mixing service, virtual currency users enter a contract to mix their virtual currency in a single transaction. Each party can send the virtual currency to themselves or another party. The transaction makes it difficult to trace the movement of the virtual currency.

Source: GAO analysis of documentation from federal and third-party entities, such as blockchain analytic firms. | GAO-22-105462

- A **peel chain** is a technique that criminals use in an attempt to conceal the source of funds, in which an individual user moves a large amount of virtual currency located at one virtual currency address through a series of transactions, transferring smaller amounts of virtual currency to a new address each time. Figure 6 depicts how peel chain works.

Figure 6: Example of How Virtual Currency Transactions Can Be Moved Through a "Peel Chain"



Source: GAO analysis of documentation from federal and third-party entities, such as blockchain analytic firms. | GAO-22-105462

Online Venues

A number of online venues, including the Surface Web, Dark Web, and Dark Web marketplaces, are used to facilitate illicit activities with virtual currency. However, officials from several agencies stated that Dark Web marketplaces are one of the most common venues that use virtual currency, as observed by these agencies. DHS officials stated that these marketplaces are dependent upon virtual currencies overall to maintain their operations. Internal Revenue Service (IRS) officials also told us that early criminal use of virtual currency often took place on the Surface Web, but criminals have increasingly moved operations to the Dark Web to evade law enforcement.

- **Surface Web:** Content on the Surface Web has been indexed by traditional search engines (e.g., Google, Bing) and is readily available

to the general public. Examples include websites for news, e-commerce, marketing, and social networking. However, illicit transactions using virtual currencies, including human and drug trafficking, can occur on both the Surface Web and Dark Web (described below), according to IRS and U.S. Postal Service (USPS) officials. For example, some virtual currency exchanges that are involved in money laundering schemes operate on the surface because they claim to be legal money service businesses, according to IRS officials. Department of Homeland Security (DHS) officials stated virtual currencies use for illicit transactions do not happen often on the Surface Web because of the increased risk for vendors to be caught and shutdown.

- **Dark Web and Deep Web:** The Dark Web is a hidden part of the Internet where specialized software (e.g., Tor) enables users to access with little risk of detection.[3] The Dark Web is a part of the Deep Web (a layer of the internet that has not been indexed by traditional search engines, such as Google) and may be used for legitimate purposes. For example, some news organizations have sites on the Dark Web that enable users to transmit information anonymously. However, some users may access the Dark Web to conceal criminal or malicious activities.
- **Dark Web marketplaces:** Dark Web marketplaces are hidden services that offer criminals a level of anonymity since they can only be accessed using specialized software (e.g., Tor) that conceals the Internet Protocol addresses of the users, which law enforcement may use to track down criminals operating on the internet. According to a 2019 advisory by FinCEN, the use of virtual currency, in combination with Dark Web market activity, may indicate the sale or purchase of drugs and other cybercrime.

[3]According to a 2017 Congressional Research Service report, “Tor” is short for “The Onion Router” and refers both to the software that a user installs on their computer and the network of computers that manages Tor connections. Congressional Research Service, *Dark Web*, CRS-7-5700 (Mar. 10, 2017).

Appendix III: Proposed Regulations to Improve Collection, Verification, and Identification of Virtual Currency Customers

The Financial Crimes Enforcement Network (FinCEN) has proposed rules that would impose greater customer identification and verification requirements at lower thresholds and increased reporting of certain virtual currency transactions. In October 2020, FinCEN issued a notice of proposed rulemaking that would amend the recordkeeping and travel rule regulations under the Bank Secrecy Act (BSA).[1] The current recordkeeping and travel rule requires banks and nonbank financial institutions to collect, retain, and transmit certain information related to funds transfers and transmittals of funds in the amount of $3,000 and more.[2] For example, financial institutions that provide money transfer services for nonestablished customers must obtain and retain specific information, such as name; address; and, if the sender is not an established customer, the Social Security number of the sender, for each transfer of $3,000 or more. The proposed rule would lower the applicable threshold from $3,000 to $250 for funds transfers and transmittals of

[1] *See* Threshold for the Requirement To Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds That Begin or End Outside the United States, and Clarification of the Requirement To Collect, Retain, and Transmit Information on Transactions Involving Convertible Virtual Currencies and Digital Assets With Legal Tender Status, 85 Fed. Reg. 68,005 (Oct. 27, 2020) (to be codified at 31 C.F.R. pts. 1010, 1020). The 2020 notice of proposed rulemaking was published jointly with the Board of Governors of the Federal Reserve System.

[2] See 31 C.F.R. § 1010.410(e). Under 31 C.F.R. § 1010.100(ddd), a "transmittal of funds" is defined as a series of transactions beginning with the transmittor's transmittal order, made for the purpose of making payment to the recipient of the order. The term includes any transmittal order issued by the transmittor's financial institution or an intermediary financial institution intended to carry out the transmittor's transmittal order. The term transmittal of funds includes a funds transfer. Under § 1010.100(w), a "funds transfer" is a series of transactions beginning with the originator's payment order, made for the purpose of making payment to the beneficiary of the order.

funds that begin or end outside the United States.[3] It would also clarify that those regulations apply to transactions above the applicable threshold involving virtual currencies.[4] Internal Revenue Service officials who conduct BSA examinations of virtual currency entities told us that the proposed rule, if finalized, would help them more consistently enforce money services businesses' (MSB) collection of customer information and address a key gap that does not currently require MSBs to collect customer information, particularly Social Security numbers, unless transactions are greater than $3,000. FinCEN officials similarly told us that, if finalized in its current form, the proposed rule would provide clarity to the industry that the regulations apply to the collection and verification of customer information by financial institutions, including MSBs transacting in virtual currency.

According to the proposed rule and FinCEN guidance, the recordkeeping and travel rules are intended to help law enforcement and regulatory authorities detect, investigate, and prosecute money laundering and other financial crimes by preserving an information trail about persons sending and receiving funds through the funds transfer system. By lowering the threshold and clarifying its application to virtual currencies, the proposed rule would permit more information to be retained for FinCEN and obtained by law enforcement on virtual currency transactions. The lower threshold is also closer in line with international anti-money laundering standards issued by the Financial Action Task Force (FATF)—which identifies a $1,000 threshold.[5] As of the end of June 2021, FinCEN was still in the process of working with relevant agencies and reviewing public

[3]The reduction in threshold is proposed for both the recordkeeping rule (that requires financial institutions to collect and retain information on certain funds transfers and transmittals of funds), and the travel rule (that requires financial institutions to transmit to other financial institutions in the payment chain information on funds transfers and transmittals of funds).

[4]The notice of proposed rulemaking proposes to clarify the meaning of "money" in relevant rules to ensure applicability to domestic and cross-border transactions involving nonlegal tender convertible virtual currency (e.g., cryptocurrency) and digital assets that have legal tender status.

[5]On June 21, 2019, FATF adopted and issued an Interpretive Note to Recommendation 15 on New Technologies that clarifies that originating and beneficiary virtual asset service providers obtain and hold accurate originator information and required beneficiary information on virtual asset transfers and make it available on request to appropriate authorities for transactions greater than $1,000. For the most recent standards, see Financial Action Task Force, *International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation, The FATF Recommendations* (Paris, France: October 2020).

comments and did not have a specific time frame for finalizing the proposed rule.

In addition, in December 2020, FinCEN issued another notice of proposed rulemaking that includes proposals to require banks and MSBs to submit reports, keep records, and verify the identity of customers in relation to transactions involving virtual currencies or digital assets with legal tender status held in wallets not hosted by a financial institution (unhosted wallets).[6] The proposed rule would require that banks and MSBs keep records of a customer's virtual currency transactions and counterparties, including verifying the identity of their customers, if a counterparty uses an unhosted or otherwise covered wallet, and the transaction is greater than $3,000. The proposal would also require the reporting of these unhosted virtual currency transactions when over $10,000 (similar to reporting requirements that are already in place for cash transactions at the same threshold). FATF also recently issued a draft guidance proposal that identified transactions from unhosted wallets as high-risk transactions and recommended similar mitigation strategies, such as the implementation of a virtual asset equivalent of a currency transaction requirement and enhanced record-keeping requirements.[7] FinCEN officials told us their proposed rule would help address the information collection gap related to transactions involving unhosted wallets (as opposed to transfers to virtual currency exchanges). However, one blockchain analytics firm reported that, although these rules address gaps in the collection of customer information, some potential drawbacks are the additional burden on financial institutions and the potential to push criminals to use unregistered peer-to-peer exchanges that are off the radar and that investigators cannot access. FinCEN extended the comment period to March 1, 2021, on this rule, and FinCEN officials told us, as of June 2021, that they are in the process of reviewing over 7,000 comments.

[6]The proposed rule applies to certain transactions involving nonlegal tender convertible virtual currency or digital assets with legal tender status and applies to both unhosted wallets or wallets hosted by a financial institution in certain jurisdictions identified by FinCEN. *See* Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 85 Fed. Reg. 83,840 (Dec. 23, 2020) (to be codified at 31 C.F.R. pts. 1010, 1020, 1022).

[7]Financial Action Task Force, *Public Consultation on FATF Draft Guidance on a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Mar. 19, 2021).

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gretta L. Goodwin at (202) 512-8777 or goodwing@gao.gov

John H. Pendleton at (202) 512-8678 or pendletonj@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Joseph P. Cruz (Assistant Director), Anne Akin and Andrew Curry (Analysts-in-Charge), Dominick Dale, Pamela Davidson, Taylor Hadfield, Eric Hauswirth, Anne Kruse, Jenna Lada, Risto Laboski, Sasan J. “Jon” Najmi, Tracie Sánchez, Verginie Tarpinian made key contributions to this report.