United States Government Accountability Office

Report to Congressional Committees

February 2022

TRAFFICKING

Use of Online Marketplaces and Virtual Currencies in Drug and Human Trafficking

Accessible Version

GAO-22-105101

GAO Highlight

Highlights of GAO-22-105101, a report to congressional committees

February 2022

TRAFFICKING

Use of Online Marketplaces and Virtual Currencies in Drug and Human Trafficking

Why GAO Did This Study

Drug and human trafficking are longstanding and pervasive problems. Federal law enforcement agencies have noted the use of online marketplaces, such as social media sites and messaging platforms, in drug and human trafficking. Further, agencies have expressed concern about traffickers' increased use of virtual currencies—that is, digital representations of value that are usually not government-issued legal tender.

The National Defense Authorization Act for Fiscal Year 2021 includes a provision for GAO to review how a range of methods and payment systems, including online marketplaces and virtual currencies, are used to facilitate drug and human trafficking.

This report examines what is known about drug and human traffickers' use of online marketplaces and virtual currencies, efforts by federal and state agencies to counter such trafficking, and benefits and challenges virtual currencies pose for detecting and prosecuting drug and human trafficking, among other objectives.

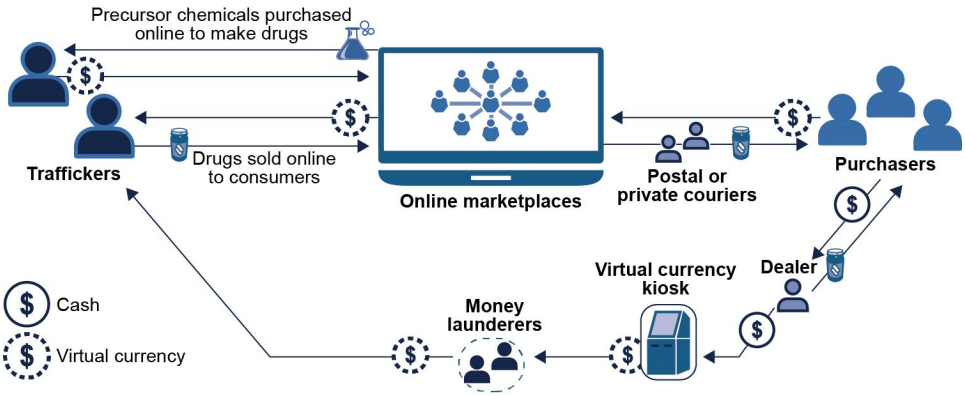
GAO reviewed federal agency and industry documentation and GAO's relevant body of past work; interviewed officials at federal and state agencies and industry and nonprofit stakeholders; and reviewed recently adjudicated cases involving the use of virtual currencies in drug or human trafficking.

View GAO-22-105101. For more information, contact Michael E. Clements at (202) 512-8678 or clementsm@gao.gov or Gretta Goodwin at (202)512-8777 or goodwing@gao.gov.

What GAO Found

Drug and human traffickers are increasingly using online marketplaces and virtual currencies to connect with buyers and obscure the source of payments, according to agency documentation and interviews with agency officials. However, according to the Department of Homeland Security, traffickers continue to primarily use cash. Online marketplaces facilitate trafficking by providing anonymity, connecting buyers and sellers, and allowing a range of payment methods, including virtual currencies (see figure). These marketplaces often use the "dark web," a hidden part of the internet that users access using specialized software. Traffickers use virtual currencies and peer-to-peer mobile payment services because transactions are somewhat anonymous, making detection by law enforcement more difficult. However, all transactions on a public blockchain (the technology used by some virtual currencies) can be tracked to some extent.

Summary of Participants Involved in Drug Trafficking Using Online Marketplaces and Virtual Currency



Source: GAO analysis of information from the Department of Justice, Drug Enforcement Administration, and Office of National Drug Control Policy. | GAO-22-105101

Several federal law enforcement agencies investigate and prosecute trafficking cases involving virtual currency and online marketplaces, including through interagency partnerships. In addition, federal regulators oversee financial institutions' processes and controls to comply with anti-money laundering requirements, including reporting of potential trafficking activities to law enforcement. State regulations such as licensing requirements for money transmitters and other virtual currency businesses also can help impede trafficking, although such requirements vary by state.

Law enforcement and others can use blockchain analytics tools to investigate suspected illicit activity that uses virtual currencies, but these tools can be of limited effectiveness. Many virtual currency transactions are permanently recorded on public blockchains, allowing them to be matched to user information collected by virtual currency platforms that comply with anti-money laundering requirements. However, law enforcement's ability to detect and track illicit uses of virtual currencies may be hindered by criminals' use of privacy technology, and by some market participants' noncompliance with anti-money laundering requirements, according to law enforcement officials and analytics firms.

Contents

Abbreviations

AML	anti-money laundering
BSA	Bank Secrecy Act
CFTC	Commodity Futures Trading Commission
COVID-19	Coronavirus Disease 2019
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
Federal Reserve	Board of Governors of the Federal Reserve System
FinCEN	Financial Crimes Enforcement Network
ICE-HSI	Immigration and Customs Enforcement's Homeland Security Investigations
IRS	Internal Revenue Service
IRS-CI	Internal Revenue Service Criminal Investigation
NCUA	National Credit Union Administration
OCC	Office of the Comptroller of the Currency
SEC	Securities and Exchange Commission
TIGTA	Treasury Inspector General for Tax Administration

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

February 14, 2022

The Honorable Sherrod Brown
Chairman
The Honorable Patrick J. Toomey
Ranking Member
Committee on Banking, Housing, and Urban Affairs
United States Senate

The Honorable Maxine Waters
Chairwoman
The Honorable Patrick McHenry
Ranking Member
Committee on Financial Services
House of Representatives

Drug and human trafficking are longstanding and pervasive problems that may be facilitated through the use of virtual currencies—digital representations of value, usually other than government-issued legal tender.[1] In addition, the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and U.S. law enforcement have observed online marketplaces being exploited or wittingly allowing their platforms to be used by criminals to further illicit activity.[2]

Anti-money laundering (AML) laws and regulations, including the Bank Secrecy Act (BSA), provide tools to help financial institutions and law enforcement detect and deter the use of financial institutions for criminal activity.[3] The BSA and its implementing regulations generally require

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

[2]For the purposes of this report, we use the term online marketplaces to mean platforms that connect individuals and facilitate transactions between them, such as social media sites, messaging platforms, e-commerce websites, and dark web marketplaces.

[3]Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114-24 (1970) (codified as amended in scattered sections of 12 U.S.C., 18 U.S.C., and 31 U.S.C.). Regulations implementing the Bank Secrecy Act primarily appear in 31 C.F.R. ch. X. For purposes of provisions of the Anti-Money Laundering Act of 2020, Bank Secrecy Act means section 21 of the Federal Deposit Insurance Act (12 U.S.C. § 1829b), chapter 2 of title I of Public Law 91–508 (12 U.S.C. §§ 1951 et seq.), and subchapter II of chapter 53 of title 31, United States Code. Pub. L. No. 116-283, div. F, title LXI, § 6003(1), 134 Stat. 3388, 4548 (2021).

financial institutions to collect and retain various records of customer transactions, verify customers' identities, maintain AML programs, and report suspicious transactions—including suspected drug and human trafficking. In addition, FinCEN has issued advisories related to drug and human trafficking and on identifying illicit activity involving virtual currencies. Federal agencies have also established interagency task forces to combat drug and human trafficking.

The National Defense Authorization Act for Fiscal Year 2021 included a provision for us to report on how a range of payment systems and methods, including virtual currencies in online marketplaces, are used to facilitate human or drug trafficking (specifically, opioids and synthetic opioids), and on the efforts of federal and state agencies to impede such activity.[4] We have issued two prior reports on federal agency efforts to counter human and drug trafficking facilitated by virtual currencies and on online platforms used for sex trafficking.[5] This report examines (1) what is known about how drug and human traffickers use online marketplaces and financial payment methods, including virtual currencies; (2) what is known about the participants that make up the supply chain or benefit from drug and human trafficking through online marketplaces or use of virtual currencies; (3) the efforts of selected federal and state agencies to counter drug and human trafficking facilitated by virtual currencies and online marketplaces; and (4) the benefits and challenges that virtual currencies and their underlying technology pose for the detection, tracking, and prosecution of drug and human trafficking.[6]

To address these objectives, we reviewed relevant federal agency reports and documentation and conducted a literature review to identify and review industry articles, research institute publications, studies, and legislative and other materials published in the past 5 years. We also reviewed reports from virtual currency analytics firms. We analyzed

[4]William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 6505(c), 134 Stat. 3388, 4630-4631 (2021).

[5]GAO, *Virtual Currencies: Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking*, GAO-22-105462 (Washington, D.C.: Dec. 8, 2021) and *Sex Trafficking: Online Platforms and Federal Prosecutions*, GAO-21-385 (Washington, D.C.: June 21, 2021).

[6]Virtual currencies and online marketplaces may be used in drug and human trafficking concurrently or separately. While virtual currencies may be used to purchase illicit goods and services through online marketplaces, they may also be used outside of online marketplaces. Likewise, online marketplaces may accept other forms of payment, such as credit cards, in addition to virtual currencies.

documentation obtained from related, ongoing GAO work and reviewed findings from GAO's body of work on online platforms, virtual currency, and trafficking. We also identified and reviewed recent drug and human trafficking court cases that involved the use of online marketplaces or virtual currencies. In addition, we interviewed officials from FinCEN, the Department of Justice (DOJ), the Department of Homeland Security (DHS), the Federal Deposit Insurance Corporation (FDIC), the Board of Governors of the Federal Reserve System (Federal Reserve), National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), the Internal Revenue Service (IRS), the Commodity Futures Trading Commission (CFTC), and the Securities and Exchange Commission (SEC). We also interviewed representatives from state financial regulators in five states (selected to reflect a diversity of regulatory approaches to virtual currency), virtual currency analytics firms, and organizations that research drug and human trafficking, among others. For more details on our scope and methodology, see appendix I.

We conducted this performance audit from March 2021 to February 2022 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.

Background

Drug Trafficking

Drug trafficking is the illicit production, transportation, or distribution of controlled substances by an individual or drug trafficking organization in violation of U.S. criminal law.[7] Nationally, rates of drug misuse have increased in recent years. Over 70 percent of the nearly 71,000 drug overdose deaths in the United States in 2019 involved an opioid, according to the Centers for Disease Control and Prevention. Synthetic opioids, such as fentanyl and fentanyl analogues, are produced in a laboratory, as opposed to opiates, such as morphine and codeine, which are derived from the poppy plant, or semisynthetic opioids, such as heroin

[7]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).

or oxycodone, which are synthesized from opium products. Illicit fentanyl produced in foreign laboratories and trafficked into the United States in powder and pill form is primarily responsible for fueling the ongoing opioid crisis. Fentanyl-laced counterfeit pills continue to be trafficked across the country and remain significant contributors to the rates of overdose deaths.[8]

According to the Drug Enforcement Administration's (DEA) 2020 *National Drug Threat Assessment*, the majority of fentanyl available in the United States is smuggled overland across the Southwest border.[9] The assessment reports that Mexican transnational criminal organizations are the greatest drug trafficking threat to the United States, in part because they control most of the U.S. drug market and have established varied transportation routes. In addition, these organizations use a combination of methods to obtain chemicals used for fentanyl production in Mexico, primarily from sources originating in China.

Human Trafficking

Human trafficking is the exploitation of a person through force, fraud, or coercion, for forced labor or commercial sex, or the exploitation of a minor by causing the minor to engage in commercial sex. Federal law generally recognizes two forms of human trafficking—sex trafficking and labor trafficking.[10] We have previously reported that the internet has enabled an

[8]Counterfeit pills are pills made to resemble other licit or illicit pills. According to the Drug Enforcement Administration, the spread of fentanyl-laced counterfeit pills in the United States is likely due to Mexican transnational criminal organizations seeking to further distribute fentanyl into prescription opioid user populations, as there is no legal production of pills containing fentanyl.

[9]Drug Enforcement Administration, *2020 National Drug Threat Assessment* (Washington, D.C.: March 2021).

[10]For the purposes of this report, human trafficking refers to "severe forms of trafficking in persons" as defined in section 103 of the Trafficking Victims Protection Act of 2000. 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 an 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, § 103(8), 114 Stat. 1464, 1470 (2000).

online market for commercial sex that may be used to promote and profit from prostitution and sex trafficking.[11]

There is no reliable estimate of the number of trafficking victims in the United States or of the money generated by this crime. However, according to Polaris (a nonprofit organization knowledgeable about human trafficking), in 2019, the U.S. National Human Trafficking Hotline was contacted 48,326 times and identified 22,326 victims and survivors of sex or labor trafficking.[12]

According to FinCEN, human trafficking generally involves three identifiable stages during which traffickers may need to interact with the financial system: recruitment or abduction, transportation, and exploitation. To supplement law enforcement efforts to fight human trafficking, FinCEN developed guidance to help financial institutions report suspicious financial activity that may be related to human trafficking.[13] In a 2020 update to that guidance, FinCEN identified alternative payment methods, including mobile payment platforms and virtual currency, as payment methods used to facilitate human trafficking.[14]

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, the Anti-Money Laundering Act of 2020 amended various definitions to include “value that substitutes for currency,” which can include virtual currency.[15]

[11]GAO-21-385.

[12]Polaris, *2019 Data Report: The U.S. National Human Trafficking Hotline* (July 2020).

[13]Financial Crimes Enforcement Network, *Advisory: Guidance on Recognizing Activity That May Be Associated with Human Smuggling and Human Trafficking—Red Flags*, FIN-2014-A008 (Sept. 11, 2014).

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

[15]Pub. L. No. 116-283, § 6102(c), 132 Stat. at 4553. The Anti-Money Laundering Act of 2020 was enacted in January 2021 as Division F of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021.

Some virtual currencies may be used to purchase goods and services from retailers that accept virtual currency as a form of payment. However, staff from FDIC said evidence of virtual currency's use as a medium of exchange for legitimate activities is limited, and officials from CFTC said most virtual currency activity consists of trading such currencies and virtual currency derivatives, and lending and borrowing such currencies for speculative purposes.[16] According to officials from several federal agencies, virtual currency can be used in a variety of crimes, including drug and human trafficking, money laundering, and cryptocurrency fraud, and as payment in ransomware attacks. As we have previously reported, the size of the virtual currency market is unknown because available data are limited; however, according to one index, the total market value of virtual currency of any type was about $2.6 trillion as of December 2021.[17]

Many virtual currencies record transactions on a blockchain. A blockchain is a type of technology made up of digital information (blocks) recorded in a public or private database in the format of a distributed ledger (chain). The ledger permanently records the history of transactions that take place among the participants within the network in a chain of encoded blocks. Blockchain analytics tools generally use machine-learning algorithms to analyze behavioral patterns and interpret information on public blockchain ledgers. Such analytics can be used by financial institutions, law enforcement agencies, and virtual currency businesses to monitor the risk of activity and track illicit uses of virtual currencies.

Virtual currency can be sent and received online through a network that can be accessed using wallet software. Virtual wallets are software programs that allow people to manage their virtual currency. Wallets do not store virtual currency like traditional physical wallets store cash. Instead, they store various components of virtual currency transactions, such as private and public keys that allow the user to gain access to the currency. Private keys are a series of alphanumeric characters that work similarly to a personal identification number or password; they prove ownership of the virtual currency and are used to sign virtual currency

[16]FDIC officials stated that "virtual currencies" is not a term used by FDIC, as demonstrated by the Joint Statement on Crypto-Asset Policy Sprint Initiative and Next Steps (Nov. 23, 2021), issued by FDIC, the Federal Reserve, and OCC, which uses the term "crypto-assets."

[17]CoinMarketCap determines the total market value (the sum of individual virtual currencies' market values) by calculating the average price of a virtual currency multiplied by the circulating supply of that virtual currency. See https://coinmarketcap.com/charts/, accessed December 2, 2021.

transactions. Public keys are a series of alphanumeric characters generated from a virtual wallet's private key that allow users to receive cryptocurrencies into their accounts.

Federal Financial Regulators

The BSA and related AML laws and regulations (collectively, BSA/AML) provide important tools used by financial institutions and law enforcement agencies to detect and deter the use of financial institutions for criminal activity, such as drug and human trafficking. As the agency responsible for administering the BSA, FinCEN issues implementing regulations and ensures financial institutions' compliance, including through imposing civil money penalties. FinCEN has delegated its authority to examine financial institutions for compliance with BSA requirements to federal regulators (see table 1).[18] Some regulators have independent authority to initiate enforcement actions against supervised institutions for violations of law and to seek civil money penalties for BSA violations.[19]

Table 1: Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Responsibilities of Selected Federal Agencies

Federal agency	Financial institutions subject to BSA/AML Requirements
Board of Governors of the Federal Reserve System (Federal Reserve)	State-chartered commercial banks that are members of the Federal Reserve System. The Federal Reserve also has authority with respect to foreign bank branches, agencies, and representative offices operating in the United States, as well as Edge Act and Agreement corporations.[a]
Office of the Comptroller of the Currency (OCC)	Nationally chartered banks and federal savings associations, as well as U.S. federally licensed offices, including branches, of foreign banks.
Federal Deposit Insurance Corporation (FDIC)	Insured state-chartered commercial banks that are not members of the Federal Reserve System, state-chartered savings associations, and insured branches of foreign-owned banks. FDIC also has back-up examination authority over insured institutions for which the Federal Reserve and OCC are the primary federal regulators.
National Credit Union Administration	Federally chartered credit unions.
Securities and Exchange Commission	Broker-dealers and mutual funds.

[18]Apart from their delegated examination authority under the BSA, the federal financial regulators and self-regulatory organizations have their own regulatory authority to examine institutions they supervise for compliance with the BSA.

[19]FinCEN, the banking regulators, and SEC may assess civil money penalties for BSA violations and take enforcement actions for noncompliance. Although CFTC has authority to examine futures commission merchants and introducing brokers in commodities, it has only limited BSA enforcement authority. IRS does not have its own separate authority to examine institutions for compliance with the BSA, with the exception of Form 8300 requirements, which are imposed under both the BSA and the Internal Revenue Code.

Commodity Futures Trading Commission	Does not directly supervise but oversees the supervision of futures and commodities brokers (introducing brokers and futures commission merchants) by the designated self-regulatory organizations (National Futures Association and CME Group).[b]
Internal Revenue Service	Nonbank financial institutions (such as money transmitters, a type of money services business).

Source: GAO analysis of agency information. | GAO-22-105101

[a]Edge Act and Agreement corporations are established as separate legal entities and may conduct a range of international banking and other financial activities in the United States. See 12 U.S.C. §§ 601-604a, 611-633.

[b]The self-regulatory organizations the Commodity Futures Trading Commission oversees are responsible for BSA/AML compliance of their members.

Much of the virtual currency activity in the United States is undertaken through intermediary financial institutions that meet FinCEN's definition of a money transmitter. Therefore, FinCEN subjects those intermediaries to regulatory requirements applicable to money services businesses, of which money transmitters are one type.[20] FinCEN has delegated BSA/AML examination authority for certain entities, including money transmitters, to IRS.

Financial institutions subject to BSA regulatory requirements are required to establish BSA/AML compliance programs, which help identify those who seek to use financial services for illicit activities. In general, financial institutions covered by the BSA must comply with the following due diligence, reporting, compliance program, recordkeeping, and other BSA/AML requirements:

- **Compliance program requirements.** Financial institutions must maintain written compliance programs that are reasonably designed to ensure and monitor compliance with the recordkeeping and reporting requirements of the BSA and that align with the institutions' money laundering and other illicit financial activity risks.[21]
- **Customer due diligence requirements.** Certain financial institutions are responsible for implementing appropriate risk-based due diligence

[20]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.

[21]31 U.S.C. § 5318(h); 12 U.S.C. §§ 1818(s), 1786(q)(1).

procedures, which include verifying customer identities and understanding the potential risks associated with their customers.[22]

- **Reporting requirements.** Financial institutions are required to submit reports to FinCEN when customer and bank activities meet certain criteria.[23] For example, banks and money services businesses are required to file suspicious activity reports 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 money services businesses and (2) the institution knows, suspects, or has reason to suspect that the transaction is suspicious.[24]
- **Recordkeeping, information sharing, and other requirements.** Financial institutions are required to maintain records for certain types of transactions, search their records when requested by FinCEN, and take targeted actions as requested.[25] For example, financial institutions are generally required to collect and retain identifying and other information for each funds transfer of $3,000 or more.[26]

Law Enforcement Agencies

Various agency components within the Department of the Treasury, DHS, and DOJ are responsible for enforcing U.S. laws and regulations related to drug and human trafficking. Broadly, these law enforcement agencies are characterized as investigative and prosecutorial agencies.

- **Investigative agencies.** Investigative agencies within DOJ include DEA and the Federal Bureau of Investigation (FBI). Within DHS, Immigration and Customs Enforcement's Homeland Security Investigations (ICE-HSI) and the U.S. Secret Service also conduct criminal investigations, such as into the illegal cross-border movement

[22]31 C.F.R. §§ 1010.220, 1010.230. In 2016, FinCEN issued a final rule requiring banks, brokers or dealers in securities, mutual funds, futures commission merchants, and introducing brokers in commodities to establish risk-based procedures for conducting customer due diligence. *See* Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29398 (May 11, 2016).

[23]31 C.F.R. §§ 1010.300–1010.370.

[24]31 C.F.R. §§ 1020.320 (reports by banks), 1022.320 (reports by money services businesses).

[25]31 C.F.R. §§ 1010.400–1010.540.

[26]31 C.F.R. § 1010.410(e), 1020.410.

of people, goods, and other contraband throughout the United States. The U.S. Postal Service's U.S. Postal Inspection Service identifies and seizes trafficked drugs that come through the postal service. IRS Criminal Investigation (IRS-CI) conducts criminal investigations into crimes such as tax crimes, money laundering, and currency violations.

- **Prosecutorial agencies**. Within DOJ, litigating divisions, such as the Criminal Division and U.S. Attorneys' offices, enforce and prosecute violations of certain federal criminal laws, including drug and human trafficking violations involving virtual currencies.[27] Furthermore, the Executive Office for U.S. Attorneys provides general executive assistance and supervision to the U.S. Attorneys' Offices. These prosecutorial components often work together to target and prosecute criminal offenses either in partnership or through programmatic support and guidance.

Federal agencies have also established interagency task forces to combat drug and human trafficking, including the Organized Crime Drug Enforcement Task Forces, as well as interagency working groups, such as the President's Interagency Task Force to Monitor and Combat Trafficking in Persons and the Senior Policy Operating Group, which consists of senior officials of the agencies on that task force.

Traffickers Can Use Online Marketplaces and Virtual Currency Technology for Illicit Activities

Traffickers Can Use Online Marketplaces as Platforms for Illicit Transactions

Drug and human traffickers can use online marketplaces to connect with buyers, allowing traffickers to promote illegal goods and services while attempting to avoid detection by law enforcement. These marketplaces can include social media websites and messaging platforms, as well as marketplaces that exist on the dark web (described below). According to FinCEN officials, those criminals who would otherwise be deterred by face-to-face transactions, risks of violence or detection, or geographic constraints can use online marketplaces for illicit transactions. According to DOJ officials, online marketplaces may enable individuals who are

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

grooming, recruiting, or advertising online to connect with possible victims without meeting with the victims in person.

Illicit activity can occur on online marketplaces operating on the surface web or the dark web. The dark web is a hidden part of the internet that users access using specialized software (e.g., Tor). In contrast, content on the surface web has been indexed by traditional search engines (e.g., Google, Bing) and is readily available to the general public and law enforcement. As we recently reported, according to IRS officials, early criminal use of virtual currency often took place on the surface web.[28] According to representatives from the Center on Illicit Networks and Organized Crime, a nonprofit organization that researches criminal networks, drug trafficking continues to occur on the surface web using traditional payment methods. However, we recently reported that criminals have increasingly moved operations to the dark web, which can provide a level of anonymity and potentially limit the risk of detection by law enforcement.[29]

Marketplaces can offer a range of payment methods, including traditional payment methods and virtual currencies. As we previously reported, the use of virtual currency as a payment method has been increasing, including on online marketplaces as payment for illicit activities.[30]

Drug Trafficking

Illicit actors have used online marketplaces to facilitate drug transactions, including the sale of opioids and fentanyl. U.S.-based individuals can purchase illicit drugs via online marketplaces and send payments in virtual currency. As reported by DOJ, virtual currency is increasingly being used to buy and sell illegal drugs on dark web marketplaces and by drug cartels to launder their profits.[31] Additionally, agencies reported that traffickers use the internet and technology to conceal their illicit activities, and their methods have become increasingly sophisticated. For example, sellers of fentanyl and other illicit synthetic opioids have leveraged online

[28]GAO-22-105462.

[29]We discuss the use of dark web marketplaces in drug trafficking in GAO-22-105462. As discussed later in this report, ICE-HSI and IRS-CI have taken actions against individuals and platforms operating on the dark web.

[30]GAO-22-105462.

[31]Department of Justice, *Cryptocurrency Enforcement Framework* (October 2020).

marketplaces to reach and transact with customers. According to representatives of the Center on Illicit Networks and Organized Crime, illicit actors may use social media to transact with customers and to target potential customers recovering from addiction. For example, drug dealers may target support groups on social media platforms with posts offering illicit drugs or counterfeit pills.

According to a 2018 U.S.-China Economic and Security Review Commission report, Chinese distributors use online marketplaces to mask their identities while reaching potential customers in the United States and around the world.[32] In an updated 2021 report, the same commission reported that various drug groups leverage password-encrypted websites and private groups on social media and messaging apps to operate online marketplaces.[33] The marketplaces are used by illicit fentanyl buyers and sellers while avoiding detection by U.S. and Chinese law enforcement. The 2021 commission report also stated that, in recent years, Chinese traffickers have increased cooperation with Mexican cartels to ship illicit drugs into the United States. Additionally, Mexican cartels are increasing their use of virtual currency because of its anonymity and the speed of transactions.

Federal prosecutors have brought criminal cases against some dark web marketplaces that facilitated the sale and purchase of illegal drugs. For example, Silk Road was a prominent dark web marketplace that used Bitcoin as payment for drug transactions. 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.[34] The website included a Bitcoin-based payment system to help conceal illicit transactions.

As trafficking-related online marketplaces have been shut down, illicit activity has moved to other online marketplaces. In December 2021, we

[32]U.S.-China Economic and Security Review Commission, *Fentanyl Flows from China: An Update Since 2017* (Nov. 26, 2018).

[33]U.S.-China Economic and Security Review Commission, *Illicit Fentanyl from China: An Evolving Global Operation* (Aug. 24, 2021).

[34]Department of Justice, “Manhattan U.S. Attorney Announces the Indictment of Ross Ulbricht, the Creator and Owner of the “Silk Road” Website,” press release no. 14-032, February 4, 2014, https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-indictment-ross-ulbricht-creator-and-owner-silk-road.

reported that as law enforcement has shut down predominant online marketplaces used for drug trafficking, a number of smaller marketplaces have emerged, as criminals have intentionally moved their operations to smaller marketplaces to avoid detection.[35] 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 their operations to other established marketplaces.

Human Trafficking

As we have previously reported, evidence suggests that virtual currency is one of several payment methods used in sex trafficking but that it may not be used as frequently in labor trafficking.[36] Illicit actors can conduct some sex trafficking financial transactions entirely online, such as through the acceptance of payment for live virtual sex shows involving trafficked individuals. Sex trafficking may also be initiated online, such as through advertisements for commercial sex where buyers can purchase sexual services provided by trafficked individuals, with services ultimately rendered in person.

Traffickers can use a variety of online platforms to solicit buyers, including social media, dating applications, and messaging platforms. In June 2021, we reported that online marketplaces have been used to promote and facilitate commercial sex markets.[37] Additionally, we reported that, according to DOJ officials, most online advertisements for commercial sex are posted on the surface web as opposed to the dark web. For example, prior to its seizure in 2018, backpage.com was the leader in the U.S. online commercial sex market for several years and an alleged platform for sex trafficking. After credit card companies stopped processing backpage.com payments, the backpage.com defendants are alleged to have accepted payment in virtual currencies, such as Bitcoin, from traffickers who sought to advertise victims for commercial sex on the website. We reported that following backpage.com's seizure in April 2018,

[35]GAO-22-105462.

[36]GAO-22-105462.

[37]GAO-21-385. The online market for commercial sex includes prostitution of oneself or others and sex trafficking. While prostitution and sex trafficking both involve commercial sexual activity, sex trafficking is defined under federal law as inherently exploitative in that it generally entails individuals being made to engage in commercial sex acts against their will. 16 U.S.C. § 1591.

some existing commercial sex market platforms suspended services in the United States, while other sites moved abroad.[38]

Traffickers Can Use Virtual Currency Technology for Illicit Transactions

Drug and human traffickers can employ virtual currencies and related technology, with or without online marketplaces, to help obscure illicit transactions and activities. Virtual currencies have been more prevalent in drug trafficking transactions than in human trafficking, according to agency officials. Data are limited on the extent to which traffickers use virtual currency to facilitate these crimes, but officials have observed increased use of virtual currencies for illicit activities, both through online marketplaces and independent of online platforms. However, while criminals can use virtual currencies and related technology for illicit activities, some characteristics of virtual currency technology can hinder their adoption.

Virtual Currency Can Have Varying Degrees of Transparency

Some anonymity-enhanced virtual currency tools can be used to help users obfuscate transactions and activities. For example, illicit actors have turned to mixers and tumblers to help maintain the anonymity of their transactions. Mixers and tumblers are centralized private services that mix the virtual currency of several users during transfers to increase anonymity.[39] 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.

Some types of anonymity-enhanced virtual currency tools, such as privacy coins, have varying degrees of transparency. Privacy coins can have technical encryption features that make it more difficult to trace or to attribute transactions. Privacy coins can conceal criminal activity and complicate the ability of law enforcement and others to trace illicit transactions. These virtual currencies are often exchanged for other virtual currencies, such as Bitcoin, in a technique commonly referred to as “chain hopping.” Chain hopping involves transferring one virtual currency

[38]GAO-21-385.

[39]According to FinCEN officials, FinCEN considers certain mixers and tumblers to be financial institutions with obligations under the BSA.

to another virtual currency on a different blockchain, often in rapid succession. Some privacy coins also have a built-in mixing capability, described above.

Despite their ability to help obscure payments, virtual currency activities are easier to trace than transactions using traditional assets such as cash, according to virtual currency analytics firms we interviewed. For example, public blockchains enable the potential tracing of transactions and participants. However, law enforcement agencies and others may still face challenges when tracing illicit activity via public blockchains, as discussed later in this report.

Virtual Currency Is Used for Both Drug and Human Trafficking

Law enforcement agencies have observed an increased use of virtual currency for illicit activities such as drug trafficking, according to federal agency officials, and evidence suggests that virtual currencies are used for certain types of human trafficking. However, we recently reported that the extent of virtual currency use for drug and human trafficking is unknown because of data limitations.[40] A significant limitation to accurately understanding the extent of drug and human trafficking activities is that perpetrators of these illicit activities purposefully try to obscure their actions, making it difficult to fully account for the number of criminal violations. We recently found that opportunities exist to enhance federal efforts to collect data for use in combating these crimes. We recommended that federal law enforcement agencies, to the extent practicable, identify and employ improved methods to consistently capture data on the use of virtual currency in human and drug trafficking.[41]

Drug trafficking. Drug traffickers have increased the use of virtual currency for illicit activities, in part because of the ability to transfer large values more readily than in the form of bulk currency and the growing adoption of virtual currencies by the general public, according to DEA's 2020 *National Drug Threat Assessment*.[42] In addition, DHS officials said travel restrictions during the Coronavirus Disease 2019 (COVID-19)

[40]GAO-22-105462.

[41]See GAO-22-105462.

[42]Drug Enforcement Administration, *2020 National Drug Threat Assessment*.

pandemic have made cash smuggling more difficult and pushed some traffickers to transfer funds using virtual currencies. However, the officials noted that the increased use of virtual currency may not have a causal relationship with the COVID-19 pandemic. As noted in our December 2021 report, officials from several federal agencies stated that drug trafficking is a common illicit use of virtual currency.[43] However, DHS officials noted that drug traffickers continue to primarily use cash. According to IRS-CI officials, the use of virtual currencies for drug trafficking is more prevalent for transactions between individual retail buyers and sellers than in large-scale trafficking transactions.

Human trafficking. As we have previously reported, evidence suggests that virtual currencies are used for sex trafficking but not as frequently for labor trafficking.[44] Platforms in the online commercial sex market, which can facilitate sex trafficking, accept a variety of traditional and alternative payment methods. In June 2021, we reported that 15 of the 27 platforms we reviewed in the online commercial sex market accepted virtual currency.[45] Credit cards and debit cards were the most accepted form of payment and were accepted by 19 of the 27 platforms.

Trafficking-Related Transactions Can Occur without Online Marketplaces

Virtual currency kiosks (also called cryptocurrency ATMs) and peer-to-peer mobile payments can also be used to facilitate trafficking-related payments without the use of online marketplaces. According to DHS officials, transnational criminal organizations can accept payment in virtual currency for drug or human trafficking activities independent of online platforms. For example, as noted in our December 2021 report, a drug dealer may receive virtual currency payments directly from a buyer and send the narcotics through the mail.[46]

Virtual currency kiosks. As we have previously reported, virtual currency kiosks can be used for illicit activity, including drug trafficking.[47]

[43]GAO-22-105462.

[44]GAO-22-105462.

[45]GAO-21-385.

[46]GAO-22-105462.

[47]GAO-22-105462.

Virtual currency kiosks are stand-alone machines that facilitate the buying, selling, and exchange of virtual currencies, including through cash payments. DHS officials noted that kiosks have been used to purchase drugs from dark web vendors. In addition, DEA's 2020 *National Drug Threat Assessment r*eported evidence of Mexican and Colombian transnational criminal organizations using virtual currency kiosks to transfer proceeds internationally. For example, money couriers deposit large volumes of cash from illegal drug proceeds into a kiosk to convert the value to virtual currency. The funds can then 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 government-issued currency, such as the U.S. dollar.

Operators of virtual currency kiosks that accept and transmit value are subject to the same registration requirements as all other money services businesses, according to FinCEN officials. We recently reported that while kiosk operators are required to register with FinCEN, they are not required to routinely report the specific locations of their kiosks. Although FinCEN can request this information from operators, a lack of routine data collection limits the data available to track and identify virtual currency kiosks. We recommended that FinCEN, in consultation with IRS, review registration requirements for virtual currency kiosk money services businesses and take appropriate actions, as needed, based on that review.[48]

Peer-to-peer mobile payments. Peer-to-peer mobile payments can provide a means of payment between individuals through transactions between personal virtual currency wallets or services such as Venmo and Paypal. Additionally, peer-to-peer mobile payments can be used to exchange virtual currencies for government-issued currency. According to FinCEN officials, the use of peer-to-peer mobile payments to facilitate sex trafficking has increased. For example, officials noted that mobile payments can be used to pay for hotels and transportation. However, according to DOJ officials, some peer-to-peer mobile payment services provide less anonymity to their users, which deters human traffickers' use of such platforms to transfer illicit funds.

[48]See GAO-22-105462 for more information. Treasury and IRS concurred with our recommendation. In response to this report, FinCEN officials said that imposing additional requirements on kiosk operators would require new regulations.

Some Characteristics of Virtual Currency Technology Can Hinder Illicit Activities

Some characteristics of virtual currency technology may limit criminals' use of virtual currency for trafficking activities. For example, representatives from a virtual currency analytics firm said that anonymity-enhanced technology can have a steep learning curve. Similarly, the Center on Illicit Networks and Organized Crime representatives said traditional financial payment methods have a lower barrier to entry and require less technological skill. However, as we recently reported, criminals continue to become more sophisticated with their use of technology.[49]

In addition, virtual currency's value can be more volatile than government-issued currency, which can create financial uncertainty. For example, DOJ officials explained that a rapid drop in the value of Bitcoin in March 2020 caused a withdrawal of many dark web vendors who feared a loss of funds if Bitcoin devalued while in escrow. (Some dark web marketplaces may hold financial payments in escrow while a vendor delivers illicit goods.) However, some virtual currencies are designed to be less volatile than others. For example, stablecoins are a type of virtual currency that purports to have less volatility than other virtual currencies.[50] As discussed later in this report, DHS officials have observed the use of stablecoins by some organizations that launder drug trafficking proceeds.

[49]GAO-22-105462.

[50]While definitions of stablecoins may differ, according to the Financial Action Task Force, stablecoins are a type of virtual currency that aims to maintain a stable value relative to an underlying asset or benchmark. For example, the value of a stablecoin may be pegged to the value of a government-issued currency or a basket of assets that may include government-issued currencies. In November 2021, the President's Working Group on Financial Markets (together with FDIC and OCC) released a report on risks and regulatory gaps related to stablecoins that can be used as a means of payment, and included recommendations for addressing those gaps. See President's Working Group on Financial Markets, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency, *Report on Stablecoins* (November 2021).

Drug and Human Trafficking Involve a Range of Participants

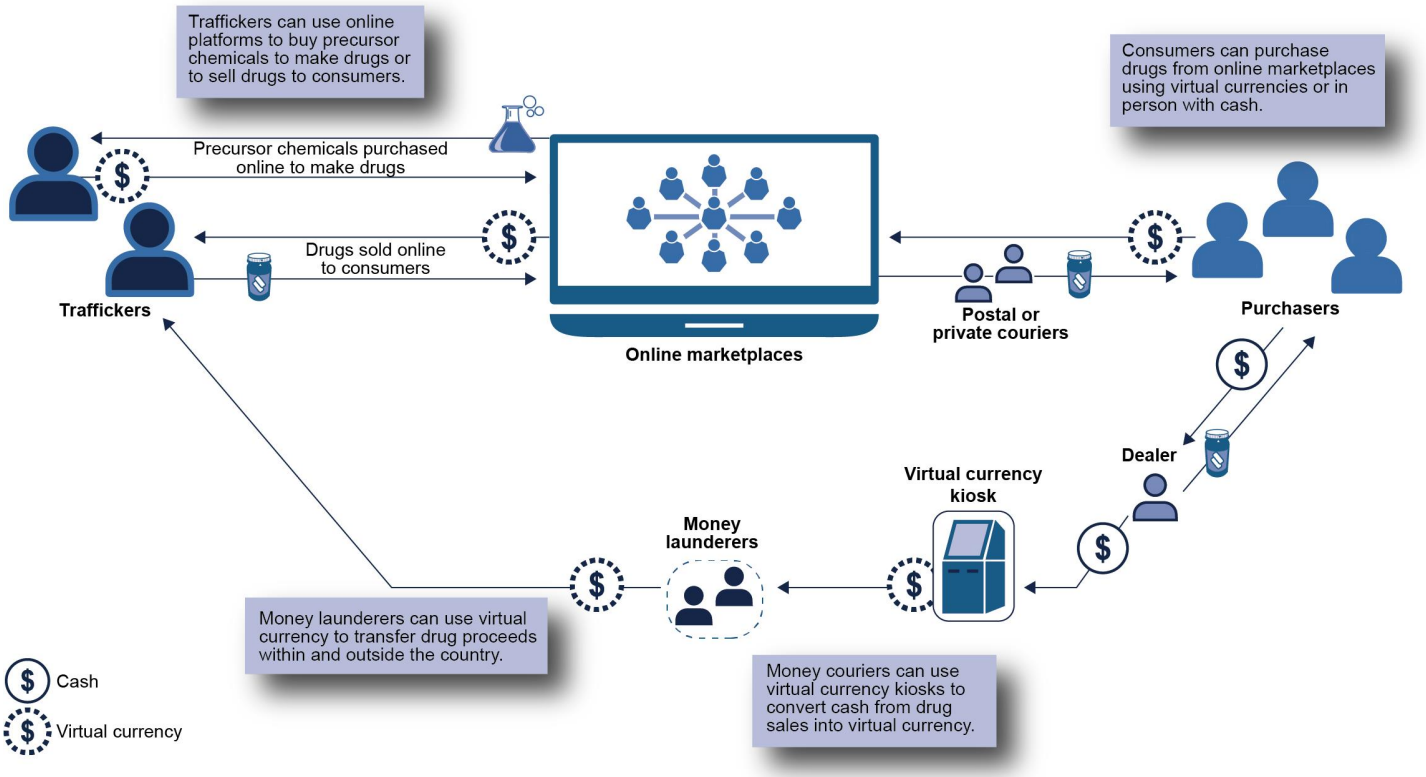
Drug Trafficking Participants Can Include Manufacturers, Marketplace Operators, and Peer-to-Peer Exchangers

According to reports from and interviews with law enforcement agencies, multiple actors make up the supply chain for drug trafficking online or using virtual currency. While most illicit drugs are purchased through interpersonal connections or on the street, the drug trafficking supply chain can use online marketplaces and virtual currencies in manufacturing and selling illicit drugs. We have previously reported that the majority of illicit drugs consumed in the United States are produced in Mexico and South America and enter the United States across the Southwest border or through the Caribbean.[51] According to DEA, transnational criminal organizations are increasingly using virtual currencies to launder the proceeds of illicit drug sales.[52] See figure 1 for a summary of participants that make up the supply chain for drug trafficking on online marketplaces and using virtual currency.

[51]GAO, *Counternarcotics: Overview of U.S. Efforts in the Western Hemisphere*, GAO-18-10 (Washington, D.C.: Oct. 13, 2017).

[52]Drug Enforcement Administration, *2020 National Drug Threat Assessment*.

Figure 1: Summary of Participants Involved in Drug Trafficking Using Online Marketplaces or Virtual Currency



Source: GAO analysis of information from the Department of Justice, Drug Enforcement Administration, and Office of National Drug Control Policy. | GAO-22-105101

Drug Traffickers

Drug traffickers, including manufacturers and dealers, use online marketplaces and virtual currency throughout the supply chain. Drug manufacturers can use virtual currencies to purchase the precursor chemicals to create illicit drugs. For example, manufacturers of synthetic opioids (including fentanyl) use online payment platforms and virtual currencies to purchase precursor chemicals or completely synthesized narcotics, which are primarily sourced from China, according to an advisory from the Office of National Drug Control Policy.[53] As previously mentioned, drug dealers can sell illicit drugs directly on online

[53]Office of National Drug Control Policy, *Advisory to Financial Institutions on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids* (Aug. 21, 2019), https://www.state.gov/wp-content/uploads/2020/02/Fentanyl-Advisory-Money-Tab-D-508.pdf.

marketplaces, including social media sites and dark web marketplaces, with or without using virtual currency.

State actors may also participate in or benefit from drug trafficking. For example, according to FinCEN officials, foreign state actors in two countries have been implicated in drug trafficking. The officials noted that while reports indicate that one of the countries mines cryptocurrency to finance illicit activities, including for trafficking of drugs such as methamphetamine, the extent to which state actors from the other country use virtual currencies in drug trafficking is unknown. In addition, according to the Congressional Research Service, DOJ has previously identified Venezuelan officials as participating directly in the activities of transnational criminal organizations related to money laundering and drug trafficking.[54]

Online Marketplace Operators

Online marketplace operators run marketplaces (or platforms) on both the surface web and dark web that can be used by participants in the drug trafficking supply chain. Surface web platforms used for drug trafficking include social media platforms, e-commerce websites, mobile applications, and online forums. As previously stated, such platforms can be used to connect buyers and sellers and to complete transactions.

In addition, foreign-based websites operate on the surface web and sell illicit drugs to buyers. For example, suppliers may present themselves as pharmaceutical companies or chemical research companies and offer fentanyl and other synthetic opioids. These suppliers market their products on websites that generally appear legitimate and have user interface features similar to legitimate e-commerce websites.[55] Some users of online pharmaceutical companies with legitimate prescriptions may not be aware that the websites they are buying from are not legitimate. According to representatives from the Center on Illicit Networks and Organized Crime, some customers seek out online suppliers for lower prescription drug prices and are often not aware that

[54]Congressional Research Service, *Venezuela: Challenges for U.S. Policymakers in 2021* (Mar. 9, 2021).

[55]Office of National Drug Control Policy, *Advisory to Digital Private Sector Platforms on Illicit Activity and Methods Related to the Marketing of Fentanyl and Synthetic Opioids* (Aug. 21, 2019), https://www.state.gov/wp-content/uploads/2020/02/Fentanyl-Advisory-Marketing-Tab-B-508.pdf.

the products they are buying are illicit or may contain dangerous substances.

Drug traffickers also use dark web marketplaces to sell illicit drugs, as discussed previously. Dark web marketplaces provide dealers with a large customer base and allow dealers to advertise their products with detailed descriptions. Such marketplaces often also have their own forums for customers to share information about different drugs, vendors' reputations, and ways to use certain virtual currencies to obfuscate their activities.[56]

Virtual Currency and Peer-to-Peer Exchangers

Various participants use virtual currency and peer-to-peer exchangers to make and receive payments for drug sales and to transfer proceeds into the banking system. According to DEA's 2020 *National Drug Threat Assessment*, virtual currency exchangers have emerged as a service to ease the conversion of government-issued currency into virtual currency, and vice versa.[57]

In addition, one analytics firm we spoke to said that peer-to-peer exchangers are a primary means of transferring funds into the U.S. banking system. According to DEA's 2018 *National Drug Threat Assessment*, traffickers can use a peer-to-peer exchanger to connect an individual who wants to convert a specific amount of virtual currency into government-issued currency with another individual who has the amount of government-issued currency needed to make the exchange.[58] The exchanger then accepts the virtual currency from the first individual and the government-issued currency from the second and makes the exchange, while taking a commission from both parties. The parties to the exchange never meet, and the government-issued funds can enter the banking system through bank deposits, online money transfer services, and other means, allowing illicit actors to launder drug proceeds.

[56]Office of National Drug Control Policy, *Advisory to Digital Private Sector Platforms*.

[57]Drug Enforcement Administration, *2020 National Drug Threat Assessment*.

[58]Drug Enforcement Administration, *2018 National Drug Threat Assessment* (Washington, D.C.: October 2018).

Money Couriers and Money Laundering Organizations

Some money couriers and money laundering organizations use virtual currency to help drug traffickers launder illicit drug proceeds and to transfer such proceeds into the banking system. Money laundering organizations use virtual currency to transfer proceeds across borders on behalf of transnational criminal organizations. For example, according to DEA's 2020 report, Asian money laundering organizations have been working with Latin American drug trafficking organizations with increasing frequency, and their methods for facilitating the movement of drug money include using virtual currencies. According to DHS officials, drug trafficking organizations can contract with professional money launderers to convert bulk cash proceeds from drug sales in the United States into virtual currency that is then sent within and outside the country. Such money launderers can use a complex web of virtual currencies, including cryptocurrency and stablecoins, and financial accounts to launder drug proceeds.

There is also some evidence that virtual currency kiosk operators can benefit from drug trafficking. For example, DEA's 2020 report explains how kiosks can sometimes be used by drug couriers, with assistance from kiosk operators. Specifically, money couriers deposit large volumes of cash into virtual currency kiosks to convert the value to virtual currency. Once the value of the original drug proceeds is in virtual form, it can easily be transferred to another virtual currency user, which allows couriers to avoid much of the risk of transporting large amounts of bulk cash. Despite kiosks being subject to federal BSA/AML reporting thresholds, kiosk owners sometimes assist in obscuring drug proceeds, according to DEA's report. Kiosks used in this manner may be unlisted and unavailable for use by the general public and instead kept hidden for exclusive use by money launderers and couriers. The cash in the machines is then integrated into the revenue stream of the owner of the kiosk.[59]

Distributers

Distributers of drugs purchased online include private and public postal carriers and street-level couriers. While street gangs dominate the retail sale and distribution of illicit drugs such as cocaine, methamphetamine, heroin, and fentanyl at the local level, drugs purchased online can also be

[59]Drug Enforcement Administration, *2020 National Drug Threat Assessment*.

shipped directly to consumers. Domestically, individuals who use the internet or local connections to buy fentanyl from U.S. suppliers typically either make payments in-person with cash or make payments in virtual currencies using money services businesses or online payment platforms and then receive a shipment directly, according to an advisory by the Office of National Drug Control Policy.[60]

Illicit synthetic opioids sourced from foreign manufacturers are typically shipped through international mail or express consignment carriers directly to the United States or are shipped to transnational criminal organizations in Mexico or Canada for later distribution.[61] Once in the United States, fentanyl may be mixed into other drugs, cut with diluents, pressed into pills, or sold as-is on the street or dark web.[62]

Human Trafficking Participants Can Include Recruiters, Marketplace Operators, and Hotels

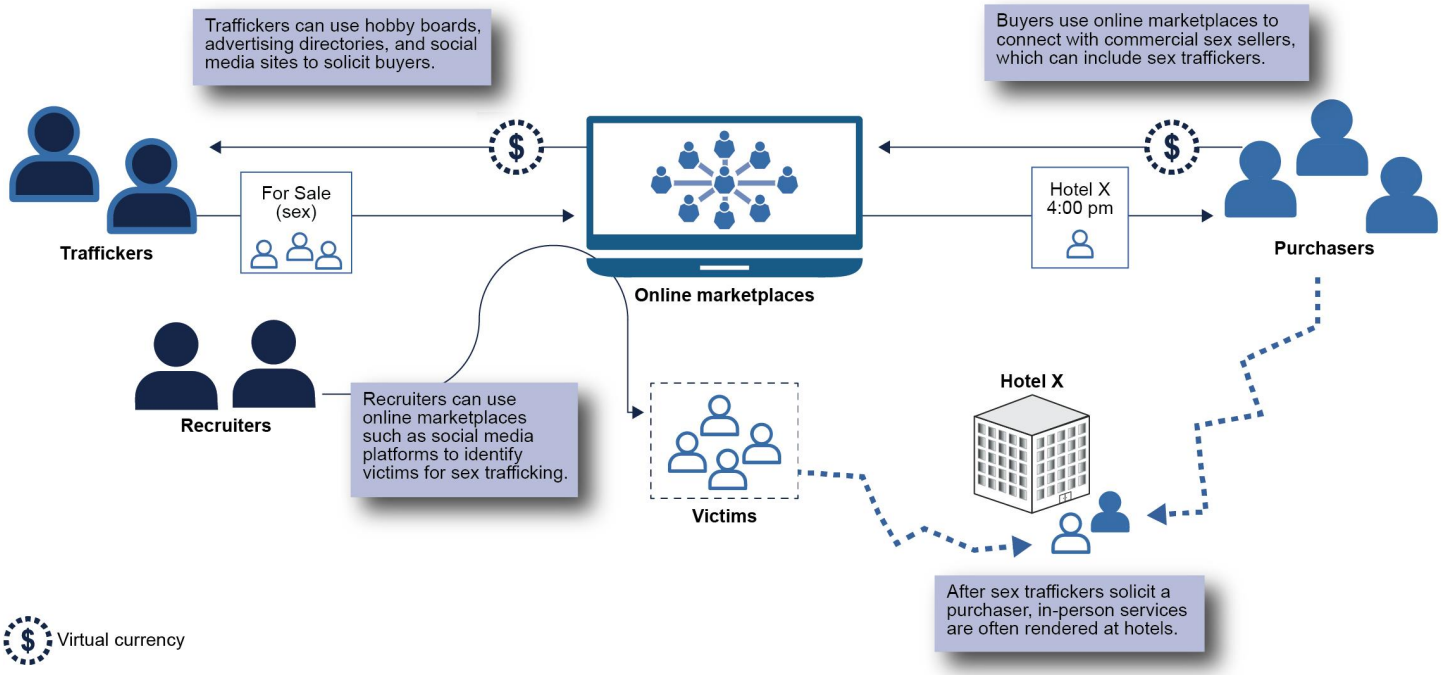
Key participants or beneficiaries of human trafficking on online marketplaces or using virtual currencies include recruiters and traffickers, online marketplace operators, and virtual currency exchange operators. As stated previously, there is evidence that virtual currency is used more often in sex trafficking than in labor trafficking, and online marketplaces can be used by traffickers to recruit victims and to connect traffickers with potential buyers (see fig. 2 for a summary of how online marketplaces and virtual currency can be used in sex trafficking).

[60]Office of National Drug Control Policy, *Advisory to Financial Institutions*.

[61]Office of National Drug Control Policy, *Advisory to the Chemical Manufacturing Industry on Illicit Activity and Methods Related to the Manufacturing of Fentanyl and Synthetic Opioids* (Aug. 21, 2019), https://www.state.gov/wp-content/uploads/2020/02/Fentanyl-Advisory-Manufacturing-Tab-A-508.pdf.

[62]Office of National Drug Control Policy, *Advisory to the Shipping Industry on the Illicit Movement Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids* (Aug. 21, 2019), https://www.state.gov/wp-content/uploads/2020/02/Fentanyl-Advisory-Movement-Tab-C-508.pdf.

Figure 2: Summary of Participants Involved in Sex Trafficking Using Online Marketplaces or Virtual Currency



Source: GAO analysis of information from Polaris, Human Trafficking Institute, and prior GAO work. | GAO-22-105101

Recruiters and Traffickers

Recruiters and traffickers use online marketplaces to identify victims and to connect with buyers. According to a 2018 Polaris report, recruiters use social media platforms to identify victims for labor and sex trafficking.[63] For example, traffickers often use social media to begin relationships with potential victims to recruit them into sex trafficking. In addition, sex and labor traffickers can recruit victims by posting fake or deceptive job offers on major social media platforms. The Human Trafficking Institute reported that, based on its review of federal sex trafficking cases between 2014 and 2019, the internet was defendants' primary method of soliciting buyers in over 80 percent of new cases.[64]

[63]Polaris, *On-Ramps, Intersections, and Exit Routes: A Roadmap for Systems and Industries to Prevent and Disrupt Human Trafficking* (July 2018).

[64]Human Trafficking Institute, *2019 Federal Human Trafficking Report* (May 2020).

Some evidence suggests that the actions of foreign state actors can facilitate human trafficking. For example, a recent report from the Department of State said that North Korean workers are sent by their government to work abroad in a range of industries, including apparel, construction, hospitality, and IT services, with their salaries appropriated by the North Korean government.[65] That report, citing nongovernmental organization reports, stated the North Korean government generates hundreds of millions of dollars annually from such trafficking. In addition, it said North Korean officials use the proceeds from state-sponsored labor trafficking to fund both government functions and illicit activity. In addition, according to FinCEN officials, North Korea's human rights violations can fuel human trafficking, as asylum seekers from North Korea are vulnerable to traffickers.

Online Platform Operators

Online platform operators run platforms that can be used for recruiting trafficking victims and connecting sellers to buyers. We have previously reported that platforms in the online commercial sex market generally fall within three broad categories:

- **Advertising.** Directories or classified services for escorts or adult entertainers can advertise on online platforms. The majority of the content on these platforms is paid advertisements for individuals or businesses providing commercial sex.
- **Hobby boards.** Hobby boards allow commercial sex buyers (self-identified "hobbyists") to review individuals or businesses providing commercial sex and participate in discussion forums on the subject.
- **Sugar dating.** These platforms connect individuals for romantic relationships under a commercial arrangement in which sexual activity may be expected or implied.[66]

[65]Department of State, *2021 Trafficking in Persons Report* (June 2021).

[66]GAO-21-385. We stated in this report that the categories of advertising, hobby board, and sugar dating are not mutually exclusive, as there may be overlap in how these platforms function and monetize their use. For instance, a hobby board platform may allow membership or advertising options to those who wish to advertise commercial sex. See app. II of that report for more information and details on these types of platforms.

As we have previously reported, online platforms for commercial sex can also facilitate sex trafficking.[67] In addition, according to Polaris, social media sites have been used in trafficking operations. For example, Polaris reported that in 2017, nearly 8 percent of active federal online sex trafficking cases prosecuted in the United States involved advertisements for sex on Facebook.[68]

Traffickers routinely establish and use front companies to hide the true nature of a business and its illicit activities, according to FinCEN.[69] Such companies are used to combine illicit proceeds with those gained from legitimate business operations. Front companies can generate revenue from sales of alcoholic beverages and cover charges, while patrons also can obtain illicit sexual services from trafficked individuals, usually elsewhere in the establishment. In addition, their social media pages can be used to assist human trafficking. For example, Polaris found that sex and labor traffickers facilitate their operations by using business pages on common social media sites to grow their customer base at legitimate venues that employ trafficked workers, such as bars and restaurants, nail salons, or landscaping services.[70]

Virtual Currency Exchange Operators

Virtual currency exchange operators can benefit from trafficking by offering one of several payment options that may be used in sex trafficking. As mentioned previously, in a June 2021 report on the online commercial sex market, we analyzed payment methods accepted by 27 platforms and found that over half (15 of 27) accepted virtual currency as a form of payment.[71] In addition, platforms in the online commercial sex market appear to be encouraging the use of virtual currency.[72] For example, a Polaris report stated that some platforms offer discounted

[67]GAO-21-385.

[68]Polaris, *On-Ramps, Intersections, and Exit Routes*.

[69]Financial Crimes Enforcement Network, *Supplemental Advisory on Identifying and Reporting Human Trafficking*.

[70]Polaris, *On-Ramps, Intersections, and Exit Routes*.

[71]GAO-21-385.

[72]GAO-22-105462.

rates to customers who pay with virtual currency.[73] This report also stated that most platforms that accept virtual currency incorporate a third-party virtual currency exchange into their payment system. Peer-to-peer exchange platforms can also be used for similar purposes. For example, according to FinCEN, human traffickers can purchase prepaid cards and then use the cards to purchase virtual currency on peer-to-peer exchange platforms. Traffickers then use the virtual currency to buy online advertisements that feature commercial sex acts to obtain customers.[74]

Hotels

Hotels can also be part of the supply chain of sex and labor trafficking. For example, hotels are frequently used by sex traffickers after soliciting a buyer online. According to the Human Trafficking Institute's review of federal human trafficking prosecutions in 2019 that involved commercial sex, 80 percent of those sex acts took place at a hotel.[75] Similarly, a Polaris survey of human trafficking survivors found that 75 percent reported contact with hotels at some point during their trafficking.[76]

Polaris's report also found labor trafficking victims in the hospitality sector, including in hotels and motels, working as front-of-house staff, food service providers, and most frequently, as housekeepers. In reviewing data from its national hotline, Polaris had difficulty ascertaining the actual employer of victims who contacted the hotline because of the complex staffing systems involved in many labor supply chains, including hospitality.

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

[74]Financial Crimes Enforcement Network, *Supplemental Advisory on Identifying and Reporting Human Trafficking*.

[75]Human Trafficking Institute, *2019 Federal Human Trafficking Report*. This count includes sex trafficking cases in 2019 in which there was a completed sex act and the location of the sex was available in public sources.

[76]Polaris, *On-Ramps, Intersections, and Exit Routes*.

Federal Agencies Counter Trafficking through Investigations and Oversight of BSA/AML Compliance

Law Enforcement Agencies Investigate and Prosecute Trafficking Involving Virtual Currencies and Online Marketplaces

Federal law enforcement agencies conduct investigations and prosecute individuals for drug and human trafficking, including when trafficking involves virtual currencies or online marketplaces.[77] Within DOJ, agencies such as DEA and FBI investigate potential trafficking activity involving these technologies, which can include tracing virtual currency addresses and subpoenaing information held by exchanges to identify suspects. In October 2021, DOJ announced the creation of a National Cryptocurrency Enforcement Team to investigate and prosecute criminal misuses of virtual currency, including for drug and human trafficking. According to DOJ, the team will support international, federal, state, and local law enforcement authorities.

Within DHS, ICE-HSI and the Secret Service also conduct criminal investigations related to trafficking. For example, in 2016 ICE-HSI—which conducts federal criminal investigations into the illegal cross-border movement of people, goods, money, and technology—investigated and seized $1.2 million in cash from an individual who sold illegal drugs via the dark web. The investigation used analytics tools to identify the individual's virtual currency wallet address. The Secret Service's financial and cybercrime investigations focus on complex financial crimes facilitated by internet-based technologies, including illicit financing operations and money laundering, according to the agency. The Secret Service has investigated and taken action against virtual currency exchangers facilitating illicit activity, including in 2017 against the virtual currency exchange BTC-e, described later in this report.

In 2015, IRS-CI established a Cyber Crime Unit, which conducts investigations of potential cybercrimes involving the use of virtual

[77]We previously reported on law enforcement efforts to counter the use of virtual currency in drug and human trafficking; see GAO-22-105462.

currencies, according to an IRS-CI report.[78] For example, IRS-CI contributed to law enforcement efforts to shut down Helix, a dark web virtual currency mixer that provided money-laundering services to customers of a dark web marketplace that facilitated drug trafficking.[79]

Law enforcement agencies use criminal statutes that relate to drug and human trafficking as the legal basis to pursue actors who use virtual currency or online marketplaces for such criminal activity. For example, in 2018 DOJ announced a 43-count indictment charging two individuals with operating a conspiracy that manufactured and shipped fentanyl and 250 other drugs to multiple countries and states, using virtual currency to launder proceeds.[80] The charges included conspiracy to manufacture and distribute controlled substances, conspiracy to import controlled substances into the United States, and money laundering.

Law enforcement agencies also use information collected by financial institutions as required by BSA/AML regulations to detect and investigate potential criminal activity involving online marketplaces and virtual currency. We previously reported that law enforcement personnel who worked on cases related to drug trafficking frequently used suspicious activity reports and other BSA reports for investigations and other purposes (74 percent). We reported that such reports were used less frequently in human trafficking cases (27 percent) (see fig. 3).[81]

[78]Internal Revenue Service Criminal Investigation, *Annual Report 2020,* IR-2020-255 (Nov. 16, 2020).

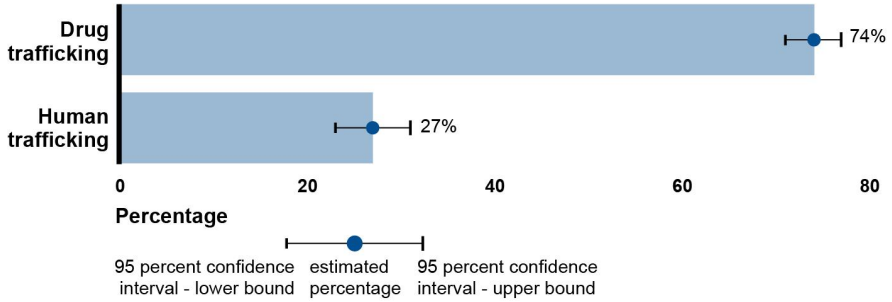
[79]In October 2020, FinCEN announced it assessed a $60 million civil money penalty against the founder and primary operator of Helix for violations of the BSA. According to FinCEN, this case represented the first Bitcoin “mixer” penalized by FinCEN for violating AML laws.

[80]Department of Justice, “Two Chinese Nationals Charged with Operating Global Opioid and Drug Manufacturing Conspiracy Resulting in Deaths,” press release no. 18-1085, August 22, 2018, https://www.justice.gov/opa/pr/two-chinese-nationals-charged-operating-global-opioid-and-drug-manufacturing-conspiracy.

[81]GAO, *Anti-Money Laundering: Opportunities Exist to Increase Law Enforcement Use of Bank Secrecy Act Reports, and Banks’ Costs to Comply with the Act Varied*, GAO-20-574 (Washington, D.C.: Sept. 22, 2020).

Figure 3: Estimated Percentage of Law Enforcement Personnel Who Reported Using Bank Secrecy Act Reports to Work on Various Crimes, 2015–2018

Survey Question: From 2015 through 2018, did you use Bank Secrecy Act (BSA) reports for your work on criminal investigations; analysis of trends, patterns, and issues associated with criminal activities; or criminal prosecutions for any of the following potential crimes?



Source: GAO survey of law enforcement agencies. | GAO-22-105101

Accessible Data Table for Figure 3

	Percentage	Lower bound	Upper bound
Drug trafficking	74	71	77
Human trafficking	27	23	31

Note: The data in this figure are taken from figure 6 in GAO, *Anti-Money Laundering: Opportunities Exist to Increase Law Enforcement Use of Bank Secrecy Act Reports, and Banks' Costs to Comply with the Act Varied*, GAO-20-574 (Washington, D.C.: Sept. 22, 2020). For that report, we surveyed 5,257 federal law enforcement personnel from six agencies responsible for investigations, analysis, and prosecutions from November 9, 2019, through March 16, 2020. The lower and upper bound of the 95 percent confidence intervals for our survey estimates are given at the left and right ends, respectively, of each whisker. Margin of error for the estimates is 4 percentage points or less at the 95 percent level of confidence.

Law enforcement agencies collaborate through partnerships and task forces related to drug and human trafficking, both domestically and internationally. For example, the Organized Crime Drug Enforcement Task Forces is an independent component of DOJ dedicated to dismantling large-scale drug trafficking, money laundering, and organized crime networks. Key member agencies include DOJ, DHS, Treasury, and state and local law enforcement agencies. According to task force officials, as of September 2020, approximately 6 percent of its investigations involved the use of virtual currency by transnational criminal organizations for sex, labor, and drug trafficking or money laundering. Law enforcement agencies also collaborate by sharing technical expertise and providing each other with forensic, intelligence, and investigative support.

FinCEN Has Taken Actions to Counter Drug and Human Trafficking, and Federal Financial Regulators Support These Efforts

FinCEN efforts to deter the use of virtual currency or online marketplaces for drug or human trafficking include issuing guidance to help financial institutions detect such activity. In addition, federal banking regulators and securities and derivatives regulators support the detection and deterrence of trafficking by issuing and enforcing BSA/AML regulations, which implement BSA/AML requirements, and, along with IRS, overseeing their supervised institutions' compliance with BSA/AML requirements.

FinCEN

FinCEN administers the BSA and issues guidance to financial institutions to help them combat illicit activity, including instances when trafficking is facilitated by virtual currency or conducted through online marketplaces. In June 2021, FinCEN established priorities for countering money laundering and terrorist financing, as required by law.[82] These priorities included crimes facilitated by virtual currency, drug trafficking, and human trafficking. Financial institutions, such as banks, covered by the BSA will be required to incorporate the priorities into their compliance programs, as appropriate, such as by assessing the potential risks associated with the priority areas as these risks relate to the services they offer or the customers they serve.[83]

[82]Pub. L. No. 116-283, § 6101(b)(2)(B)(ii), 134 Stat. at 4551 (codified at 18 U.S.C. § 5318(h)(4)(A); Financial Crimes Enforcement Network, *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities* (June 30, 2021).

[83]The AML Act requires that, within 180 days of the establishment of the anti-money laundering and countering the financing of terrorism (AML/CFT) priorities, the Financial Crimes Enforcement Network shall promulgate regulations regarding the AML/CFT priorities. 18 U.S.C. § 5318(h)(4)(D). The AML Act also requires financial institutions, such as banks, to incorporate the AML/CFT priorities into their BSA compliance programs after the effective date of the final revised regulations. Federal banking regulators announced they plan to revise their BSA regulations to address how the priorities will be incorporated into banks' BSA requirements. See Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency, and state bank and credit union regulators, *Interagency Statement on the Issuance of the Anti-Money Laundering/Countering the Financing of Terrorism National Priorities* (June 30, 2021).

FinCEN also receives and analyzes suspicious activity reports about illicit activities such as trafficking. Financial institutions, such as banks and virtual currency exchanges, are generally required to file suspicious activity reports with FinCEN if they know, suspect, or have reason to suspect that a transaction may involve illicit activity.[84] FinCEN's suspicious activity report form allows financial institutions to include narrative information where they may indicate a suspicion of drug trafficking, and it includes a checkbox for institutions to flag if the financial activity is suspected to be associated with human trafficking. FinCEN is also responsible for collecting and analyzing financial intelligence information received from financial institutions and sharing such analysis with federal, state, local, and foreign law enforcement agencies.

FinCEN provides information to help financial institutions better detect suspicious activity. For example, FinCEN issued an advisory to financial institutions to help them identify illicit financial schemes related to the trafficking of fentanyl, including how criminals use virtual currency to buy fentanyl in online marketplaces and to anonymize their transactions.[85] This guidance provided indicators to help financial institutions identify suspicious activity, such as transactions with dark web marketplaces or virtual currency mixing services. Advisories also include reporting instructions, such as using key words, which enable FinCEN and law enforcement to more efficiently analyze BSA data, according to FinCEN officials.

FinCEN's enforcement division conducts BSA compliance investigations both proactively and as a result of referrals from financial regulators' examinations, and it uses dissuasive measures to enforce compliance with the BSA, according to the agency. According to FinCEN officials, if a financial institution, such as a virtual currency exchange, violates the BSA, FinCEN may take civil action against it. FinCEN officials also said they have observed an increase in virtual currency exchanges registering with FinCEN as money services businesses and filing suspicious activity reports. This improves the security of the financial system and provides

[84]31 C.F.R. §§ 1020.320, 1022.320. Virtual currency exchanges generally qualify as money transmitters under the BSA, according to FinCEN guidance.

[85]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).

law enforcement with more financial intelligence, according to FinCEN officials.

FinCEN is responsible for coordination and information-sharing activities, such as leading the BSA Advisory Group, the main BSA coordination mechanism among regulators, law enforcement, and industry. Through the BSA Advisory Group, stakeholders communicate about how law enforcement uses suspicious activity and other BSA reports and how reporting requirements can be improved to enhance their utility while minimizing costs to financial institutions.

Banking Regulators

Federal banking regulators do not focus specifically on combatting drug and human trafficking, according to agency officials.[86] Rather, federal banking regulators examine their supervised institutions' compliance with BSA/AML requirements and regulations, which impose a range of recordkeeping and reporting obligations on banks and credit unions.[87] In complying with BSA/AML requirements, financial institutions assist in the detection and prevention of illicit activity by maintaining effective internal controls—such as retaining transaction records—and reporting suspicious activity.

Banks and credit unions are subject to BSA/AML requirements when providing virtual currency-related services.[88] OCC has issued a number of interpretive letters addressing the authority of national banks to engage in virtual currency-related services. In the letters, OCC concluded that national banks have the authority to provide certain virtual currency-related services, including providing virtual currency custody services on behalf of customers and holding U.S. dollar deposits serving as reserves backing stablecoin in certain circumstances.[89] As stated in the letters,

[86]For the purposes of this report, we are defining federal banking regulators to include OCC, NCUA, the Federal Reserve, and FDIC.

[87]Federal banking regulators have issued regulations establishing procedures to monitor their supervised institutions' compliance with BSA/AML requirements. *See* 12 U.S.C. §§ 1786(q), 1818(s).

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

[89]Office of the Comptroller of the Currency, *Interpretive Letter #1170: Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers* (July 2020).

banks providing these virtual currency-related services must comply with BSA/AML requirements, including by conducting customer due diligence with respect to account holders and reporting suspicious activity.[90] Identifying the owner of an account can help law enforcement investigations and impair criminals' ability to anonymously use banks to engage in illicit activity, according to FinCEN.

Federal banking regulators oversee financial institutions' compliance with BSA/AML requirements through examinations. A key function of examinations is to assess whether examined institutions have established the appropriate policies, procedures, and processes to comply with the BSA and identify and report suspicious activity, including financial activity associated with drug or human trafficking. Banks and credit unions base their BSA/AML compliance programs on their specific money laundering and other illicit financial activity risk. FDIC officials said examinations are informed in part by a bank's independent risk assessment and review for compliance with AML requirements. If a bank has identified a customer as higher risk, FDIC examiners might include that specific customer in transaction testing performed as part of a BSA/AML examination.

Examinations may include reviews of virtual currency transactions if the institution or its customers participate in such activity, although this is not a particular focus since a limited number of banks participate in such activities, according to officials from federal banking regulators. Officials from some regulators said it was unlikely that examinations, which focus on compliance with regulatory requirements and are not investigations, would uncover trafficking activity and that this information was more likely to be found in financial institutions' suspicious activity reports. For example, OCC officials said examiners conduct transaction testing to evaluate the effectiveness of bank processes in identifying suspicious activity without focusing on specific topologies or crimes, such as human trafficking. Identifying human trafficking activity through financial transactions and activity is complex and requires in-depth investigation, according to the officials.

Officials from banking regulators explained that their agencies would take relevant regulatory and enforcement actions if a bank or credit union did not have a reasonably designed BSA/AML compliance program or if there

[90]Office of the Comptroller of the Currency, *Interpretive Letter #1179: Chief Counsel's Interpretation Clarifying: (1) Authority of a Bank to Engage in Certain Cryptocurrency Activities; and (2) Authority of the OCC to Charter a National Trust Bank* (November 2021).

were failures in a part of the BSA/AML compliance program, including having ineffective controls to detect and report suspicious or illicit financial activity as required by the BSA. Examinations and enforcement help ensure that banks and credit unions implement effective BSA/AML programs, including risk-based processes for identifying and reporting suspicious activity, which may include activity relating to drug or human using virtual currency or online marketplaces.

Securities and Derivatives Regulators

SEC and CFTC issue regulations implementing BSA/AML requirements and are responsible for overseeing BSA/AML compliance of virtual currency businesses and online marketplaces in certain circumstances. In 2019, CFTC, SEC, and FinCEN issued a joint statement reminding people engaged in virtual currency activity that the nature of virtual currency activity determines with what agency the institution must register and therefore how it is regulated.[91] For example, in a 2021 congressional testimony, the SEC chair said most virtual currency exchanges are likely to offer tokens that meet SEC's definition of a security, given the hundreds of virtual currencies offered on these platforms.[92] Like the banking regulators described above, the securities and derivatives regulators and their self-regulatory organizations oversee their supervised institutions' compliance with BSA/AML requirements through risk-focused examinations, which supports detecting, investigating, and deterring trafficking activity.[93]

While SEC and CFTC do not focus specifically on combating drug and human trafficking, both agencies have indicated that misconduct involving virtual currency is a key priority for examinations and enforcement, and

[91]Commodity Futures Trading Commission, Securities and Exchange Commission, and Financial Crimes Enforcement Network, *Leaders of CFTC, FinCEN, and SEC Issue Joint Statement on Activities Involving Digital Assets* (Oct. 11, 2019).

[92]Gary Gensler, Chair of the Securities and Exchange Commission, *Oversight of the U.S. Securities and Exchange Commission,* testimony before the Senate Committee on Banking, Housing, and Urban Affairs. 117th Con. 1st session, Sept. 14, 2021.

[93]Self-regulatory organizations are nongovernmental entities that regulate their members through the adoption and enforcement of rules and regulations governing business conduct subject to agency oversight. Self-regulatory organizations for the securities and derivatives industries—including the Financial Industry Regulatory Authority and the National Futures Association—have BSA/AML responsibilities and conduct BSA examinations of their members. SEC and CFTC oversee the examinations conducted by self-regulatory organizations.

they have taken actions against noncompliant virtual currency businesses. For example, in August 2021, a federal court entered a consent order against the entities operating the BitMEX platform—which offers trading of virtual currency derivatives—in response to charges filed by CFTC. The order found, among other violations, that BitMex failed to implement compliant anti-money laundering and customer identification programs.[94] According to FinCEN, BitMEX conducted at least $209 million worth of transactions with known dark web markets or virtual currency mixers, which can anonymize illicit transactions.

IRS

FinCEN has delegated authority to IRS to examine certain nonbank financial institutions not covered by other federal financial regulators for compliance with BSA/AML requirements. These entities include money services businesses, some of which may pose trafficking and money-laundering risks due to their large volume of transactions.[95] According to Treasury's *National Strategy for Combating Terrorist and Other Illicit Financing*, much virtual currency activity is conducted by entities that meet FinCEN's definition of money transmitters, a type of money services business that accepts and transmits funds or virtual currency from one person or location to another.[96] For example, virtual currency exchanges—which exchange virtual currency for government-issued currency, funds, or other virtual currency—generally qualify as money transmitters under the BSA, according to FinCEN guidance. As of October 2021, over 24,000 money services businesses were registered with FinCEN, of which 13,093 were money transmitters, according to our analysis of FinCEN data.

As with the federal banking regulators, IRS examinations may help deter trafficking activity—including activity involving virtual currencies or online marketplaces—by ensuring money services businesses have effective

[94]Consent Order for Permanent Injunction, Civil Monetary Relief, and Other Equitable Relief, CFTC v. HDR Global Trading, 1:20-cv-08132 (S.D.N.Y. Aug. 10, 2021).

[95]For more information on the risks posed by these money services businesses, see GAO, *Bank Secrecy Act: Examiners Need More Information on How to Assess Banks' Compliance Controls for Money Transmitter Accounts*, GAO-20-46 (Washington, D.C.: Dec. 3, 2019).

[96]Department of the Treasury, *National Strategy for Combating Terrorist and Other Illicit Financing* (Feb. 6, 2020). FinCEN regulations include a definition of money transmitters. *See* 31 C.F.R. § 1010.100(ff)(5).

BSA/AML programs. If an IRS BSA examiner determines that a money services business has engaged in potential violations of the BSA or criminal activity, IRS-CI may investigate the case, or the case may be referred to FinCEN, which may issue a civil penalty.

Treasury and the Treasury Inspector General for Tax Administration (TIGTA), which provides independent oversight of IRS, have identified challenges related to IRS's oversight of money services businesses. Treasury identified money services businesses as a key vulnerability in its *National Strategy for Combating Terrorist and Other Illicit Financing*.[97] Specifically, Treasury cited challenges with money transmitters that do not implement AML requirements and with IRS's ability to maintain enough examinations and examiners. TIGTA has noted weaknesses with IRS's oversight of virtual currency businesses. For example, in 2020, TIGTA reported that IRS examined few virtual currency businesses, which represented slightly more than 1 percent of total BSA examinations in fiscal year 2020.[98]

IRS generally relies on FinCEN for formal civil enforcement action because IRS does not have authority to impose penalties, but TIGTA reported that IRS did not make a significant number of referrals to FinCEN for BSA violations. TIGTA made a number of recommendations, including that IRS and FinCEN improve coordination on referrals or that FinCEN give IRS authority to issue penalties. For the purposes of this report, we did not independently assess IRS's capacity to examine virtual currency businesses or the effectiveness of its examinations.

IRS officials said they were working to improve coordination with FinCEN. Specifically, IRS officials said they launched an effort to identify challenges and best practices related to the process for referring cases to FinCEN, and that as of February 2021 this effort was ongoing. IRS has also taken steps to increase its examinations of virtual currency businesses, including training additional examiners on virtual currency topics and contracting with blockchain analytics firms to identify unregistered money services businesses, according to IRS officials. The number of BSA compliance examinations IRS completed has generally increased since it began conducting examinations in fiscal year 2015,

[97]Department of the Treasury, *National Strategy*.

[98]Treasury Inspector General for Tax Administration, *The Internal Revenue Service Can Improve Taxpayer Compliance for Virtual Currency Transactions*, 2020-30-066 (Sept. 24, 2020).

from four in fiscal year 2015 to 21 in fiscal year 2020, with a total of 66 BSA examinations completed from fiscal years 2015 through 2020.

State Financial Regulators' Enforcement of Licensing and BSA/AML Requirements Can Help Deter Trafficking, but State Regulatory Approaches Can Vary

State financial regulators regulate and supervise state-chartered banks, and most also regulate a variety of nonbank financial services providers, including money services businesses. Officials from state financial regulators we interviewed said their agencies do not focus their activities specifically on human or drug trafficking.[99] Rather, the regulators help deter illicit activity by enforcing state licensing, registration, and examination requirements for the entities they supervise, including BSA/AML requirements, according to industry associations.

Some states have established regulations addressing virtual currency businesses and activity, which may help combat drug and human trafficking. For example, state agencies generally regulate money transmission licensing and perform supervision, which helps prevent the use of money transmitter services for illicit activities such as drug trafficking, according to a report by the Conference of State Bank Supervisors and the Money Transmitter Regulators Association.[100] According to that report, to become licensed by a state as a money transmitter, entities must provide evidence of a BSA/AML compliance program, which includes policies, procedures, and internal controls to detect and deter money laundering and other illegal activity. However, the types of activities that require licenses vary by state, including whether the transmission of virtual currency requires a license.

State financial regulators review their supervised institutions' compliance with BSA/AML requirements, including through examinations. Some state financial regulators coordinate their examinations of money services businesses because these businesses often operate in multiple states. For example, according to a 2019 report, 47 licensed virtual currency

[99]We interviewed state financial regulators from California, Massachusetts, Montana, New York, and Wyoming.

[100]Conference of State Bank Supervisors and Money Transmitter Regulators Association, *The State of State Money Services Businesses Regulation and Supervision* (Washington, D.C.: May 2016).

businesses conducted business in an average of 28 states each.[101] These coordination efforts allow examiners to cover more companies without additional personnel, according to a Treasury report.[102]

Two of the five state regulators we reviewed have developed approaches to regulating virtual currency that may help deter its use in drug or human trafficking, although their efforts do not focus on trafficking specifically.[103]

- The New York Department of Financial Services issued a regulation in 2015 requiring the license or charter of entities engaging in virtual currency business activities in the state.[104] The regulation contains provisions that address the detection and prevention of suspected fraud. Guidance published by the New York Department of Financial Services in 2018 requires regulated virtual currency entities to notify the department immediately upon detection of illicit activities, whereas FinCEN requires financial institutions to file suspicious activity reports within 30 days after detection. This could allow officials to respond quickly to suspicious activity.
- The Wyoming Division of Banking supervises and examines special purpose depository institutions, which may provide custody services for customers' digital assets, such as virtual currency. Wyoming banking officials developed a custom examination manual for these institutions based on the Federal Financial Institutions Examination Council's BSA/AML examination manual, which federal and state banking regulators use to examine banks for BSA/AML compliance.[105]

[101]Data from the Nationwide Multistate Licensing System, which is operated by the Conference of State Bank Supervisors and tracks licenses across 44 states. See Conference of State Bank Supervisors, *2019 NMLS Money Services Businesses Report*, accessed August 4, 2020, https://nationwidelicensingsystem.org/about/Reports/2019%20MSB%20Annual%20Report.pdf.

[102]Department of the Treasury, *National Strategy*.

[103]For the purposes of this report, we did not attempt to identify all approaches to regulating virtual currency by state financial regulators that could help deter human or drug trafficking. The following two states are provided as illustrative examples. Officials from the other states we reviewed—California, Massachusetts, and Montana—said their agencies conducted limited oversight of virtual currency activity.

[104]23 NYCRR Part 200.

[105]The Financial Institutions Examination Council is a federal interagency body that prescribes uniform principles, standards, and report forms for the federal examination of financial institutions by its member agencies and makes recommendations to promote uniformity in the supervision of financial institutions. 12 U.S.C. §§ 3301–3311.

Wyoming Division of Banking officials said the division's special purpose depository institutions manual is more specific to virtual currency activities than the Federal Financial Institutions Examination Council manual. The division expects special purpose depository institutions to implement controls to deter illicit activity involving virtual currency—for example, they are required to use blockchain analytics tools to identify illicit activity from their customers.

Virtual Currency Technology Can Be Used to Identify Illicit Actors, but Some Challenges Limit Transparency

Blockchain Technology Can Allow Law Enforcement and Others to Track Virtual Currency Activity and Identify Illicit Actors

Through the use of commercial analytics tools, the blockchain—the underlying technology of virtual currencies—can allow law enforcement to investigate funds suspected to be associated with illicit activity.[106] As noted previously, many virtual currency transactions are recorded on a blockchain, which is a type of technology made up of digital information (blocks) recorded in a public or private database in the format of a distributed ledger (chain). Blockchain ledgers permanently record the history of transactions that take place among the participants within the network in a chain of encoded blocks. Generally, analytics tools use machine-learning algorithms to analyze behavioral patterns, interpret information on public blockchain ledgers, and create large databases of transactions that can be used to identify activity associated with a specific virtual currency wallet. In conducting investigations, law enforcement can use these tools to trace the origin and destination of virtual currency funds by connecting seemingly anonymous transactions to wallet addresses and known entities. For example, investigators can use blockchain analytics tools to help trace transactions with dark web marketplaces (see text box). Blockchain analytics firms also provide software for virtual currency businesses to monitor for suspicious transactions on their platforms, such as interactions with known illicit wallet addresses or dark

[106]Aside from commercially available tools, some tools to analyze blockchain activity are publicly available. For example, one blockchain analytics company we interviewed offers a publicly available tool that serves as a free search engine for the Bitcoin blockchain.

web marketplaces, which they then could refer to law enforcement for investigation in support of their BSA/AML compliance obligations to report suspicious activity.

Law Enforcement Use of Blockchain Analytics Tools: The Case of Welcome to Video

In October 2019, the Department of Justice (DOJ) announced the seizure and takeover of Welcome to Video, one of the largest websites for child sexual abuse materials, which were purchased and sold using Bitcoin on the dark web.[a]

According to a report by a blockchain analytics firm, federal law enforcement agencies used a commercial analytics tool to trace Bitcoin transactions on the Welcome to Video website, examine the flow of funds from user accounts, and determine the location of the dark web server. Law enforcement was able to trace user transactions to virtual currency exchanges compliant with Bank Secrecy Act requirements and subpoena user information held by the exchanges to identify individuals behind the illicit activity.

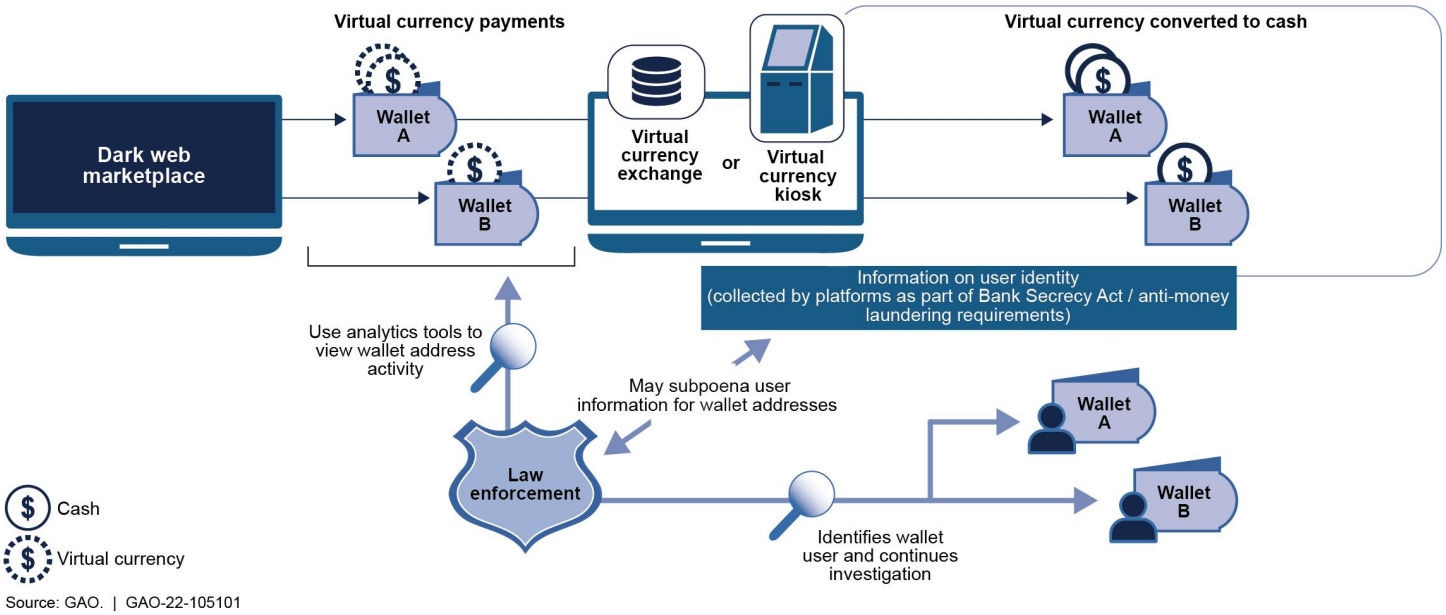
This investigation was conducted by DOJ's Criminal Division, the U.S. Attorney's Office for the District of Columbia, Internal Revenue Service Criminal Investigation, and Immigration and Customs Enforcement's Homeland Security Investigations.

Source: GAO analysis of DOJ and Chainalysis documentation. | GAO-22-105101

[a]This case is not an example of drug trafficking or human trafficking, but is included to illustrate law enforcement's use of blockchain analytics tools to identify illicit actors.

The transparency of public blockchain activity is a key benefit for tracking and identifying illicit actors, according to federal law enforcement officials and representatives of three blockchain analytics firms and one exchange. Additionally, representatives of one analytics firm and one exchange noted that the immutable nature of transactions recorded on the blockchain is also a key benefit for tracking illicit activity. Law enforcement may use analytics tools to trace funds to virtual currency platforms, such as exchanges and kiosks that are compliant with FinCEN regulations. As previously discussed, virtual currency exchanges and kiosks are generally considered to be money services businesses under FinCEN regulations and are required to collect information on the identity of their users as part of BSA/AML requirements. Once illicit actors convert virtual currency funds to government-issued currency through a BSA/AML-compliant exchange or kiosk, law enforcement may subpoena information from the platform on the identity of the user behind the activity (see fig. 4).

Figure 4: Illustrative Example of Using Public Blockchain Activity to Investigate Illicit Actors



Source: GAO. | GAO-22-105101

As previously mentioned, FinCEN officials told us they have observed more virtual currency exchangers registering with FinCEN as money services businesses and filing suspicious activity reports. This trend may assist law enforcement with investigations by allowing them to issue subpoenas to more exchanges to collect information on users' identity.

Certain Technologies and Noncompliance with BSA/AML Requirements Can Impede Investigation of Illicit Use of Virtual Currencies

Blockchain technology allows for virtual currency activity to be traced and analyzed, but some challenges exist that may limit transparency into blockchain activity and pose barriers to law enforcement investigations, such as privacy-enhancing technology and unregistered virtual currency platforms.

Privacy-Enhancing Technology

Illicit actors may use technologies that obscure the movement of funds across the blockchain, such as mixers and privacy coins, which can limit law enforcement's ability to trace illicit funds.

- **Mixers and tumblers.** Mixers and tumblers are centralized private services that mix the virtual currency of several users during transfers to increase anonymity. However, in some cases, analytics tools can trace the movement of funds to and from a mixer and analyze behavioral patterns to identify the wallet addresses associated with the activity.[107] For example, exchanges may use analytics tools to observe funds entering and leaving a mixer, and these funds may then be traced to a virtual currency exchange for conversion to government-issued currency, which may be flagged as suspicious activity by the exchange, according to representatives of a virtual currency exchange. According to a 2020 report by a blockchain analytics firm, mixers were the most popular cash-out destination for illicit funds.[108]
- **Privacy coins.** While popular virtual currency coins such as Bitcoin record transactions on public blockchain ledgers, some coins have embedded privacy technology that limits the traceability of their activity. For example, privacy coins such as Monero can use technical encryption features that make it more difficult to trace or attribute transactions.[109]

  While Monero has a privacy-encryption feature and operates on a nonpublic blockchain, other coins have varying privacy features; one coin has an optional privacy setting that users can configure to allow for its traceability, and another coin operates on a public blockchain but has an optional "PrivateSend" feature that automatically mixes transactions. According to IRS-CI officials, most U.S. exchanges only accept popular coins such as Bitcoin and Ethereum rather than privacy coins, making it difficult for illicit actors to exchange privacy coins for government-issued currency on those platforms. Representatives of two analytics firms and one exchange also noted that illicit actors use privacy coins less frequently, as they are more difficult to obtain and are supported by fewer exchanges compared to Bitcoin, making it difficult to convert funds to government-issued currency.

[107]In addition to tracing funds to and from mixers to identify actors, law enforcement may also subpoena transaction data from mixers that hold this information to identify illicit actors behind the activity.

[108]Chainalysis, *Who's Who on the Blockchain? The Chainalysis Guide to Cryptocurrency Typologies* (2020).

[109]According to a blockchain analytics firm we interviewed, the most popular coins with embedded privacy technology include Monero, Dash, and Z-Cash.

Privacy-enhancing technology is constantly evolving, and illicit actors quickly adapt to new technologies and strategies to launder funds, according to representatives of two blockchain analytics firms and federal law enforcement officials. Representatives of two analytics firms and one exchange we interviewed noted that efforts to investigate illicit uses of virtual currency may be limited by a lack of resources and expertise among some law enforcement agencies and financial regulators to monitor virtual currency activity and emerging technologies. DHS officials told us the technology used to evade law enforcement and regulators is frequently changing and becoming more complex, making it challenging for law enforcement to keep up. However, according to ICE-HSI officials, the agency's agents and analysts routinely coordinate with virtual currency analytics firms for training, webinars, and discussions of criminal typologies.

Unregistered Virtual Currency Platforms

Virtual currency platforms that operate in the United States but are not registered with FinCEN or do not comply with BSA/AML requirements can create challenges to law enforcement investigations.

Virtual currency exchanges and kiosks. U.S. market participants that are subject to FinCEN regulations but do not comply can limit law enforcement's ability to identify illicit actors.[110] Virtual currency platforms that conduct business wholly or substantially in the United States that do not register with FinCEN or comply with relevant BSA/AML requirements may face enforcement action for operating as an unlicensed money services business (see text box). While commercial analytics tools allow law enforcement to trace the movement of funds, efforts to identify illicit actors during the course of an investigation largely rely on user-identity information collected by compliant platforms.[111]

[110]As noted previously, under FinCEN guidance, virtual currency platforms, such as exchanges and kiosks, are generally considered to meet the definition of nonbank money transmitters and are therefore subject to BSA/AML requirements. As part of these requirements, such platforms must collect information on the identity of their customers and establish procedures to respond to requests from law enforcement.

[111]Law enforcement may also obtain information on the identity of illicit actors through seizures of data from dark web marketplaces that have been shut down, according to IRS-CI officials. For example, investigators may accumulate a record of all activity that occurred on the seized platform and analyze completed transactions, including whether funds were taken to an exchange, to identify the individuals behind the activity.

Enforcement Action against BTC-e Exchange

BTC-e was a virtual currency exchange operating and maintaining servers in the United States. From 2011 to 2017, BTC-e received over $4 billion worth of Bitcoins. In 2017, BTC-e was alleged to be operating as an unlicensed money services business and to be facilitating an international money laundering scheme that resulted in a $110 million civil penalty from the Financial Crimes Enforcement Network (FinCEN). BTC-e was allegedly used to facilitate a variety of criminal activities, including identity theft, drug trafficking, and helping to launder criminal proceeds.

The investigation was conducted by the Department of Justice Criminal Division, Internal Revenue Service Criminal Investigation, Immigration and Customs Enforcement's Homeland Security Investigations, the Federal Bureau of Investigation, U.S. Secret Service, the Federal Deposit Insurance Corporation, and the Department of the Treasury's FinCEN.

Source: GAO analysis of Department of Justice and FinCEN documentation. | GAO-22-105101

Available data are limited on the number of noncompliant virtual currency platforms, such as exchanges and kiosks, that operate in the U.S. market. However, as previously discussed, we recently recommended that FinCEN, in conjunction with IRS, review registration requirements for virtual currency kiosks and require operators to submit kiosk locations upon money services business registration, which could help provide FinCEN and IRS with a more complete understanding of virtual currency kiosks and ensure they are complaint with BSA/AML requirements.[112]

Decentralized exchanges. Decentralized virtual currency exchanges operate without a traditional central entity or administrator, and they are used to trade one type of virtual currency for another. According to representatives of an analytics firm we interviewed, decentralized exchanges present barriers to identifying illicit actors because no individuals or legal entity behind the platform collects and holds information on users' identities. However, according to representatives of another analytics firm, centralized exchanges are used more frequently than decentralized exchanges, as illicit users need to interact with centralized exchanges to convert virtual currency funds to government-issued currency. The representatives noted that while this may change in the future, law enforcement is currently able to continue investigations that involve decentralized exchanges because such investigations often lead to exchanges that are compliant with BSA/AML requirements.

Peer-to-peer exchangers. Individual exchangers who buy and sell virtual currency are also known as peer-to-peer exchangers. Peer-to-peer exchangers are generally considered money services businesses under FinCEN guidance and are required to comply with BSA/AML

[112]Treasury and IRS concurred with our recommendation. See GAO-22-105462 for more information. In response to this report, a FinCEN official said that imposing additional requirements on kiosk operators would require new regulations.

requirements (see text box). However, unregistered peer-to-peer exchangers who do not collect information on the identity of their users may limit law enforcement's ability to subpoena information on the identity of illicit actors. According to representatives of a blockchain analytics firm that works with law enforcement, FinCEN's guidance stating peer-to-peer exchangers are generally required to register as money services businesses and comply with BSA/AML requirements has been helpful for investigations because law enforcement can subpoena information from these platforms.

FinCEN Action against an Unregistered Peer-to-Peer Exchanger

In 2019, the Financial Crimes Enforcement Network (FinCEN) issued a civil money penalty to Eric Powers, who was found to be operating as an unregistered virtual currency exchanger. From December 2012 to September 2017, Powers admitted to conducting over 1,700 transactions as a peer-to-peer exchanger, which involved selling and purchasing Bitcoin to and from other individuals. FinCEN's investigation also found that Powers was aware of relevant Bank Secrecy Act requirements and participated in conversations about registering as a money services business, but did not do so. Powers also processed numerous suspicious transactions without filing a suspicious activity report, including conducting business related to a dark web marketplace, according to FinCEN.

This was FinCEN's first enforcement action against a peer-to-peer virtual currency exchanger.

Source: GAO analysis of FinCEN documentation. | GAO-22-105101

International platforms. Law enforcement can experience challenges in investigating potential illicit activities on international virtual currency platforms that operate in the United States. Under FinCEN regulations, an international platform qualifies as a money services business if it conducts business as such wholly or substantially in the United States, and would be required to comply with BSA/AML requirements.[113] However, such exchanges often do not comply with BSA/AML requirements, according to a 2019 FinCEN advisory.[114] FinCEN officials told us it may be difficult to get international platforms, such as exchanges, to accept subpoenas because they are typically not in one central location but dispersed globally and across jurisdictions. Additionally, because of this jurisdictional variability, some international platforms may claim they are not subject to U.S. regulations, such as BSA/AML requirements. However, FinCEN officials noted they use information from open source data and public blockchains, as well as information from law enforcement agencies and BSA reporting, to identify international exchanges that may be subject to BSA/AML requirements.

[113]31 C.F.R. § 1010.100(ff).

[114]Financial Crimes Enforcement Network, *Advisory on Illicit Activity Involving Convertible Virtual Currency*, FIN-2019-A003 (May 9, 2019).

Agency Comments

We provided a draft of this report to CFTC, DHS, DOJ, FDIC, the Federal Reserve, FinCEN, IRS, NCUA, OCC, and SEC for their review and comment. In its comment letter (reproduced in appendix II), NCUA acknowledged our findings and stated its commitment to ensuring credit unions comply with BSA/AML laws and regulations. CFTC, DHS, DOJ, FDIC, OCC, and SEC provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Chairman of the Commodity Futures Trading Commission, the Secretary of the Department of Homeland Security, the Attorney General, the Acting Chairman of the Federal Deposit Insurance Corporation, the Chair of the Board of Governors of the Federal Reserve System, the Acting Director of the Financial Crimes Enforcement Network, the Commissioner of the Internal Revenue Service, the Chairman of the National Credit Union Administration, the Acting Comptroller of the Currency, the Chair of the Securities and Exchange Commission, and other interested parties. 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 Michael Clements at (202) 512-8678 or clementsm@gao.gov or Gretta Goodwin at (202) 512-8777 or goodwing@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

Michael E. Clements
Director, Financial Markets and Community Investment

Gretta L. Goodwin
Director, Homeland Security and Justice

Appendix I: Objectives, Scope, and Methodology

Our objectives were to examine (1) what is known about how drug and human traffickers use online marketplaces and financial payment methods, including virtual currencies; (2) what is known about the participants that make up the supply chain or benefit from drug or human trafficking through online marketplaces or using virtual currencies; (3) the efforts of selected federal and state agencies to counter drug and human trafficking facilitated by virtual currencies and online marketplaces; and (4) the benefits and challenges that virtual currencies and their underlying technology pose for the detection, tracking, and prosecution of drug and human trafficking.

To address our first objective, we reviewed prior GAO reports related to drug and human trafficking and conducted a literature search to identify studies that describe the use of online marketplaces and virtual currency for drug or human trafficking published in the past 5 years.[1] The literature search included government reports, industry articles, research institute publications, and legislative materials. In addition, we interviewed officials from the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), the Internal Revenue Service (IRS), the Department of Justice (DOJ), and the Department of Homeland Security (DHS) on how online marketplaces and financial payment methods such as virtual currencies may be used to facilitate drug or human trafficking.

To address our second objective, we reviewed reports from federal agencies and offices, including the Drug Enforcement Administration (DEA), the Department of State, and the Office of National Drug Control

[1]GAO, *Virtual Currencies: Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking*, GAO-22-105462 (Washington, D.C.: Dec. 8, 2021) and *Sex Trafficking: Online Platforms and Federal Prosecutions*, GAO-21-385 (Washington, D.C.: June 21, 2021).

Policy.[2] In addition, we reviewed reports from organizations knowledgeable about drug or human trafficking, including Polaris and the Human Trafficking Institute.[3] We also interviewed the following organizations knowledgeable about trafficking or virtual currency to gain their perspectives: the Center on Illicit Networks and Organized Crime, the Blockchain Alliance, and Coin Center.

To address our third objective, we reviewed agency information and regulatory guidance from FinCEN, the federal banking regulators, and law enforcement agencies. We also reviewed relevant prior reports from GAO and the Treasury Inspector General for Tax Administration, which provides independent oversight of IRS. We also reviewed materials gathered for ongoing GAO work and prior GAO reports on federal financial regulators' implementation of the Bank Secrecy Act (BSA).[4] To describe the efforts of selected state financial regulators, we selected five states (California, Massachusetts, Montana, New York, and Wyoming) active in regulating or otherwise overseeing online marketplaces and virtual currencies, which we identified through a review of state laws or regulations related to the use of virtual currencies and online marketplaces for drug and human trafficking. These states were selected to represent a diversity of regulatory approaches to virtual currency. We reviewed relevant information from these states and interviewed officials from their financial regulatory agencies. We also interviewed representatives of the Conference of State Bank Supervisors and the North American Securities Administrators Association, which represent state financial regulators.

To address our fourth objective, we reviewed documentation from federal law enforcement agencies, such as DOJ's Cryptocurrency Enforcement

[2]For example, Drug Enforcement Administration, *2020 National Drug Threat Assessment* (Washington, D.C.: March 2021) and Office of National Drug Control Policy, *Advisory to Financial Institutions on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids* (Aug. 21, 2019), https://www.state.gov/wp-content/uploads/2020/02/Fentanyl-Advisory-Money-Tab-D-508.pdf.

[3]Polaris, *On-Ramps, Intersections, and Exit Routes: A Roadmap for Systems and Industries to Prevent and Disrupt Human Trafficking* (July 2018) and Human Trafficking Institute, *2019 Federal Human Trafficking Report* (May 2020).

[4]GAO, *Anti-Money Laundering: Opportunities Exist to Increase Law Enforcement Use of Bank Secrecy Act Reports, and Banks' Costs to Comply with the Act Varied*, GAO-20-574 (Washington, D.C.: Sept. 22, 2020) and *Bank Secrecy Act: Examiners Need More Information on How to Assess Banks' Compliance Controls for Money Transmitter Accounts*, GAO-20-46 (Washington, D.C.: Dec. 3, 2019).

Framework and guidance issued by FinCEN on registration requirements for virtual currency businesses. In addition, we interviewed federal law enforcement agencies and financial regulators on ways virtual currencies and their underlying technology may be used to identify and prosecute illicit funding. We also reviewed reports by virtual currency analytics firms to obtain information on virtual currencies and the blockchain, including developments in illicit uses of virtual currencies and crime typologies.

We judgmentally selected five virtual currency analytics firms to interview, chosen in part because they partner with U.S. government agencies on investigations and training, and operate in the United States. We also judgmentally selected three virtual currency exchanges, identified through ongoing GAO work on related topics, and chosen because they had the biggest market capitalization by asset size and activity. Although we contacted three exchanges for interviews, we only received responses from one. Information obtained from interviews cannot be generalized to all U.S. virtual currency analytics firms and exchanges. We also reviewed materials gathered for ongoing GAO work and prior GAO reports on federal efforts to combat illicit uses of virtual currencies.[5] Finally, we reviewed adjudicated cases compiled as part of ongoing GAO work to describe examples of illicit uses of virtual currencies and platforms found to be noncompliant with relevant FinCEN registration and BSA/anti-money laundering requirements.

For all objectives, we interviewed officials from FinCEN, which is responsible for the administration of the BSA, and the agencies that oversee BSA compliance. These agencies are the federal banking regulators—the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System, the National Credit Union Administration, and the Office of the Comptroller of the Currency—as well as IRS, the Commodity Futures Trading Commission, and the Securities and Exchange Commission. We also interviewed officials from federal law enforcement agencies—specifically, DEA, DOJ, and DHS—which pursue investigations and prosecutions of crimes involving drug and human trafficking facilitated by virtual currency and online marketplaces.

We conducted this performance audit from March 2021 to February 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain

[5]GAO-22-105462 and GAO, *Virtual Currencies: Additional Information Reporting and Clarified Guidance Could Improve Tax Compliance*, GAO-20-188 (Washington, D.C.: Feb. 12, 2020).

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.

Appendix II: Comments from the National Credit Union Administration

National Credit Union Administration
Office of the Executive Director

January 20, 2022

Michael E. Clements
Director, Financial Markets & Community Investment
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Clements,

We reviewed GAO's draft report (GAO 22-105101) entitled *Trafficking - Use of Online Marketplaces and Virtual Currencies in Drug and Human Trafficking.* We acknowledge GAO's observations in the draft report. The NCUA remains committed to ensuring credit unions comply with anti-money laundering and Bank Secrecy Act laws and regulations.

Thank you for the opportunity to review and comment on the draft report.

Sincerely,

LARRY FAZIO Digitally signed by LARRY FAZIO Date: 2022.01.19 12:53:16 -05'00'

Larry Fazio
Executive Director

1775 Duke Street – Alexandria, VA 22314-3428 – 703-518-1175

Agency Comment Letter

Text of Appendix II: Comments from the National Credit Union Administration

Page 1

January 20, 2022

Michael E. Clements
Director, Financial Markets & Community Investment
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Clements,

We reviewed GAO's draft report (GAO 22-105101) entitled *Trafficking - Use of Online Marketplaces and Virtual Currencies in Drug and Human Trafficking.* We acknowledge GAO's observations in the draft report. The NCUA remains committed to ensuring credit unions comply with anti-money laundering and Bank Secrecy Act laws and regulations.

Thank you for the opportunity to review and comment on the draft report.

Sincerely,

Larry Fazio Executive Director

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Michael E. Clements at (202) 512-8678, or clementsm@gao.gov

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

Staff Acknowledgments

In addition to the contacts named above, Kevin Averyt (Assistant Director), Joseph P. Cruz (Assistant Director), Shannon Smith (Analyst-in-Charge), Anna Blasco, Risto Laboski, Efrain Magallan, Marc Molino, Paris Nguyen, Jennifer Schwartz, Tyler Spunaugle, Andrew J. Stephens, Farrah Stone, and Verginie Tarpinian made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548

Please Print on Recycled Paper.