U.S. Department of
JUSTICE

U.S. Department of Justice
Washington, DC

The Report of the Attorney General Pursuant to Section 5(b)(iii) of Executive Order 14067:

The Role Of Law Enforcement In Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets

Office of the Attorney General
Washington, D. C. 20530

September 6, 2022

Dear Mr. President,

Pursuant to Section 5(b)(iii) of your March 9, 2022, Executive Order, *Ensuring Responsible Development of Digital Assets*, I am pleased to transmit the attached Report on the role of law enforcement in detecting, investigating, and prosecuting criminal activity related to digital assets. This report builds on a prior one submitted in June 2022, pursuant to the same Executive Order, detailing our efforts to expand cooperation with international partners to combat the cross-border threats related to digital assets.

As your Executive Order recognizes, the growing use of digital assets in the global financial system demands strong steps to reduce the risk that digital assets are used for illicit finance or other criminal purposes – such as money laundering, cybercrime, ransomware, narcotics, theft and fraud, and human trafficking – or to undermine our national security by enabling terrorism and proliferation financing. The Department of Justice and our law enforcement and regulatory partners are committed to protecting the public from criminal actors in the digital assets ecosystem and to meeting the unique challenges posed by developments in digital asset technologies.

In a collaborative effort between the Department of Justice, the Department of the Treasury, and the Department of Homeland Security, with significant input from several regulatory agencies, this Report details the substantial steps already taken by departments and agencies to combat the illicit use of digital assets. The Report acknowledges, however, that the success of our efforts will ultimately depend on the applicable legal and regulatory frameworks keeping pace with rapidly changing technology. The Report thus includes legal and regulatory recommendations on how to further strengthen our ability to detect, investigate, prosecute, and otherwise disrupt criminal activity.

The Department will be unwavering in its dedication to disrupt digital assets-related criminal activity, and I look forward to working with our interagency partners to use all tools at our disposal to help protect consumers, investors, and businesses from illicit activity, and promote the responsible development of digital assets.

Respectfully,

Merrick B. Garland
Attorney General

cc: The Hon. Janet Yellen, Secretary of the Treasury
The Hon. Alejandro Mayorkas, Secretary of Homeland Security
The Hon. Gary Gensler, Chair of the Securities and Exchange Commission
The Hon. Rostin Behnam, Commissioner of the Commodity Futures Trading Commission

Table of Contents

I. INTRODUCTION AND EXECUTIVE SUMMARY

On March 9, 2022, the President issued an Executive Order on Ensuring Responsible Development of Digital Assets (hereinafter Executive Order). Section 5(b)(iii) of the Executive Order directed the Attorney General to submit a report on the role of law enforcement in detecting, investigating, and prosecuting criminal activity related to digital assets, and further directed that the report "shall include any recommendations on regulatory or legislative actions, as appropriate." The Attorney General now issues that report (the Report), in an effort led by the Department of Justice's National Cryptocurrency Enforcement Team (NCET), in consultation with the Secretary of the Treasury (Treasury) and the Secretary of Homeland Security (DHS), and with input from multiple federal regulatory agencies.

The Department of Justice (Department) has previously reported on law enforcement's efforts in the digital assets space. In 2018, the initial report of the Attorney General's Cyber-Digital Task Force described how criminals were increasingly using one class of digital assets—virtual currencies—to advance their illicit activities and conceal their earnings, explained steps the Department was taking to trace transactions and seize ill-gotten gains, and recommended that the Department continue to evaluate the threats posed by cryptocurrencies.[1] Two years later, the Cyber-Digital Task Force published the *Cryptocurrency Enforcement Framework*, a report that chronicled categories of illicit uses of cryptocurrency by malicious actors, identified legal authorities and partnerships the Department had relied upon to combat criminal and national security threats involving cryptocurrency, and discussed approaches for addressing the public safety challenges related to cryptocurrency.[2]

More recently, in June 2022, the Attorney General submitted to the White House a report under Section 8(b)(iv) of the Executive Order on how to strengthen international law enforcement cooperation for detecting, investigating, and prosecuting criminal activity related to digital assets.[3] This *International Law Enforcement Cooperation Report* detailed the features of digital asset transactions that differentiate them from traditional financial transactions and explained how those features may affect transnational investigations; described several ways in which U.S. law enforcement agencies and regulators have responded to the challenges posed by cross-border digital asset investigations; and concluded with recommendations to bolster enforcement and improve international cooperation. The *International Law Enforcement Cooperation Report* also contained annexes that, among other things, described recent international training efforts conducted by federal law enforcement agencies and regulators, and provided multiple examples of cross-border investigations involving digital assets in which cooperation between U.S. law enforcement agencies and their foreign counterparts was integral to success.

This Report is a companion to the *International Law Enforcement Cooperation Report* and serves as an update to the *Cryptocurrency Enforcement Framework*. Following a structure similar to that of the *Cryptocurrency Enforcement Framework*, Part II of this Report delineates three principal categories of illicit uses of digital assets, with an added focus on an area—decentralized finance, or DeFi—that has gained prominence since 2020. Part II also includes case studies of successful law enforcement efforts to

investigate, prosecute, and otherwise disrupt digital asset crimes in spite of the investigative challenges. Part III of this Report describes initiatives that the Department and other law enforcement agencies have established to more effectively detect, investigate, prosecute, and otherwise disrupt crimes relating to digital assets, and to seize and forfeit those assets that constitute ill-gotten gains. In Part IV, this Report addresses the Executive Order's request for recommendations on appropriate regulatory and legislative actions. It proposes actions designed to enhance law enforcement's ability to gather evidence and prosecute crimes; strengthen certain laws and penalty provisions that play an important role in digital asset prosecutions; support proposed regulations that would enhance customer-identification efforts and other anti-money-laundering requirements under the Bank Secrecy Act; and ensure that law enforcement and regulatory agencies have adequate resources to conduct the technologically sophisticated investigations inherent in the digital assets space.

II. TAXONOMY OF CRIMINAL ACTIVITY RELATED TO DIGITAL ASSETS

The Department's 2020 *Cryptocurrency Enforcement Framework* detailed many of the ways illicit actors have exploited digital assets, cryptocurrencies foremost among them. As explained below, much of the criminal activity today continues to fall within the three main categories identified in the *Enforcement Framework*, but the rise of DeFi has created new opportunities for criminal exploitation—and associated challenges for law enforcement agencies investigating possible wrongdoing.

A brief note on terminology: previous Department reports have referred to "virtual currencies" or "cryptocurrencies,"[4] while relevant Treasury regulations use the term "convertible virtual currencies," or CVCs.[5] At the same time, international bodies such as the Financial Action Task Force (FATF) articulate their standards in terms of "virtual assets" and describe entities that exchange such assets as "virtual asset service providers," or VASPs.[6] Consistent with the Executive Order, this Report uses the phrase "digital assets" as an umbrella term to describe the entire class of assets at issue, adopting the definition of that term set forth in the Executive Order.[7] The most common category of digital assets involved in law enforcement investigations remains cryptocurrencies, which the Executive Order defines as "a digital asset, which may be a medium of exchange, for which generation or ownership records are supported through a distributed ledger technology that relies on cryptography, such as a blockchain."[8] References to "cryptocurrency" in Part II below and throughout this Report bear that definition.

A. Criminal Exploitation of Digital Assets

While digital assets have legitimate uses, their unique features—particularly the lack of financial intermediation, immutable and rapid settlement of transactions, and use of pseudonymous addresses—have been exploited by criminals engaged in illegal activity online. Even before the advent of cryptocurrency, criminals adopted earlier forms of digital currency (such as E-Gold and Liberty Reserve) as a medium of exchange for buying and selling drugs and other illegal goods.[9] The rise of the Bitcoin network paralleled the development of Silk Road, AlphaBay, and other illegal online marketplaces, often hosted anonymously on the "darknet," the sections of the Internet that are not indexed by search engines and that require special software to access, such as the Tor network (described below). Ancillary services sprung up to facilitate this underground economy and allowed criminals to "cash out" their illegal profits: from the use of "mixers" or "tumblers" to launder money, to unlicensed cryptocurrency exchanges that enabled anonymous or pseudonymous transactions, either through a central exchange or peer-to-peer transactions. Criminal exploitation of digital assets—and law enforcement and regulatory action to counter it—thus focused from the outset on illicit online markets.

As cryptocurrency has become more widely adopted and the digital assets space has rapidly diversified, the ways in which criminal actors exploit digital assets have multiplied. The *Cryptocurrency Enforcement*

Framework broadly divided the criminal exploitation of digital assets into three categories: (1) cryptocurrency as a means of payment for, or manner of facilitating, criminal activity; (2) the use of digital assets as a means of concealing illicit financial activity; and (3) crimes involving or affecting the digital assets ecosystem. In the two years since the publication of that *Enforcement Framework*, the digital assets ecosystem has expanded in key ways, driven by quickly evolving technology, the proliferation of digital assets beyond bitcoin,[10] and the rise of DeFi. This rapid development has given rise to new categories of criminal activity that require more coordination in government enforcement.

1. Cryptocurrency and Other Digital Assets as a Means of Payment For, or Manner of Facilitating, Criminal Activity

Cryptocurrency continues to be widely used as a medium of payment for completing illegal transactions online. Criminals rely on, among other factors, the perceived anonymity of cryptocurrency to buy and sell illegal drugs, to advertise and promote human trafficking, to collect ransomware payments, to perpetrate frauds and thefts against consumers and investors, and to finance threats to national security—including terrorist fundraising and malicious rogue state activity.

Darknet markets—which facilitate the exchange of cryptocurrency for criminal purposes—remain a significant focus of law enforcement efforts. These markets are typically accessible through the Tor network, which anonymizes Internet traffic through a global network of relay computers. Darknet markets and other illicit sites traffic in drugs, child sexual abuse material, illegal firearms, counterfeit or stolen identification documents, and stolen credit card numbers, as well as "tools of the trade," such as hacking tools and services that criminals use to facilitate further illegal activity. Transactions occur using a growing variety of cryptocurrencies, including anonymity-enhanced cryptocurrencies (AECs) or so-called "privacy coins."

HYDRA AND GARANTEX

The Hydra case is a recent example of the Department's efforts to take down darknet marketplaces and bring their operators to justice in collaboration with domestic and overseas partners.

On April 5, 2022, the Department announced the seizure of Hydra Market, the world's largest and longest-running darknet marketplace, and criminal charges against Dmitry Olegovich Pavlov, the Russian national who allegedly administered Hydra's servers since the site's creation in November 2015.[11] Hydra enabled mostly Russian-speaking users to buy and sell illegal drugs and other illicit goods and services, such as stolen financial information, fraudulent identification documents, and hacking tools and services using cryptocurrency. In fact, Hydra accounted for an estimated 80 percent of all darknet market-related cryptocurrency transactions in 2021, and until its shutdown, the marketplace had received approximately $5.2 billion in cryptocurrency. Hydra also provided an in-house mixing service to launder bitcoin, and Hydra sellers themselves often offered an array of money laundering and so-called "cash-out" services that allowed Hydra users to convert their bitcoin into other forms

of currency. Some users even set up shell accounts for the sole purpose of moving money through Hydra's bitcoin wallets as a laundering technique.

The Hydra investigation benefitted from the cooperation of multiple domestic and foreign government agencies, including with the German Federal Criminal Police (the Bundeskriminalamt), who carried out the seizure of the Hydra servers and cryptocurrency wallets containing $25 million worth of bitcoin.

The same day that law enforcement took down Hydra, the Department of the Treasury's Office of Foreign Assets Control took three related actions: (1) imposed sanctions on Hydra; (2) publicly identified more than 100 virtual currency addresses associated with the entity's operations that had been used to conduct illicit transactions; and (3) imposed sanctions on Garantex, a virtual currency exchange formerly registered in Estonia, for operating or having operated in the financial services sector of the Russian Federation economy. Analysis revealed that more than $100 million in known Garantex transactions were associated with illicit actors and darknet markets, including approximately $2.6 million from Hydra.[12]

The Hydra investigation illustrates the Department's commitment to a multi-agency, cross-border approach to identifying and disrupting unlawful activities involving cryptocurrency.

Cryptocurrency is also the payment method of choice for ransomware and other digital extortion activities. In 2021, the Federal Bureau of Investigation (FBI) received through its Internet Crime Complaint Center alone 3,729 ransomware-related complaints with adjusted losses of more than $49.2 million.[13] Reported incidents almost certainly form a small percentage of actual ransomware attacks, as estimates of global ransomware payments range into the hundreds of millions of dollars.[14] Ransomware operators have recently targeted critical infrastructure sectors—especially healthcare and public health, financial services, and information technology—which has necessitated a resource-intensive and focused Department response.[15] In May 2021, a ransomware attack led Colonial Pipeline to take offline a gasoline and jet fuel pipeline for several days, causing fuel shortages in several areas of the country, including multiple airports. The attackers demanded and received a ransom paid in bitcoin, but the Department mobilized an innovative and quick-moving investigation to successfully recover the majority of the cryptocurrency ransom.[16]

Cryptocurrency is also used to raise funds for terrorist organizations and other nation state threat actors, although cases involving cryptocurrencies are less prevalent than those involving traditional financial assets.[17] For instance, in 2020, the Department announced the government's largest-ever seizure of cryptocurrency in the terrorism context. This action disrupted al-Qassam Brigades, al-Qaeda, and ISIS (Islamic State) fundraising campaigns, including a scheme in which ISIS attempted to exploit the COVID-19 pandemic by operating a fraudulent website purporting to sell N95 masks and other personal protective equipment.[18] And in 2018, the Department charged twelve members of the GRU, a Russian Federation intelligence agency, with committing federal crimes intended to interfere with the 2016 U.S. presidential

election. The indictment alleged that the defendants attempted to avoid detection by, among other things, funding the operation with cryptocurrency earned by mining bitcoin.[19]

Rogue states have also turned to cryptocurrency theft in an effort to raise funds. The United States and the United Nations have implicated the Democratic People's Republic of Korea (DPRK), for example, in a number of cryptocurrency heists and other related criminal activity.[20] In March 2022, Lazarus Group, a hacking group sponsored by the DPRK, stole over $600 million from a blockchain project linked to an online gaming platform.[21] Regulatory actions taken in response to this theft are discussed in Part III below.

2. Cryptocurrency and Other Digital Assets as a Means of Concealing Illicit Financial Activity

Criminals continue to use cryptocurrency and other digital assets for money laundering, facilitating tax evasion, and evading sanctions. Criminals have developed increasingly sophisticated obfuscation techniques—complex and rapid transactions, "chain-hopping" by converting funds from one cryptocurrency into another, use of AECs, and other measures—designed to make tracing difficult and to place stolen funds beyond recovery. Criminals can also use mixers and tumblers, including automated services that employ smart contracts[22] to combine multiple users' coins together before sending out unrelated coins to each user's designated recipient, to obfuscate their transactions.[23]

These techniques are made easier by the fact that many digital asset exchanges and platforms make little or no effort to comply with anti-money laundering regulations, such as know-your-customer (KYC) requirements, or operate in jurisdictions without anti-money-laundering and countering-the-financing-of-terrorism (AML/CFT) requirements in line with the international standards. Under U.S. law (including the Bank Secrecy Act (BSA) and its implementing regulations), many exchanges and other participants in the digital assets marketplace qualify as money transmitters required to comply with the AML/CFT obligations that apply to money services businesses (MSBs).[24] Yet criminals continue to take advantage of noncompliant actors—including noncompliant cryptocurrency exchanges, peer-to-peer exchangers, or automated cryptocurrency kiosks—to exchange their cryptocurrency for cash or other digital assets without facing rigorous AML/CFT scrutiny. As discussed in the *International Law Enforcement Cooperation Report*, the ability to access online exchanges located in jurisdictions with less robust AML/CFT regulations and supervision than in the United States allows for criminals to engage in jurisdictional arbitrage to launder their illegal proceeds.[25] New forms of high-value digital assets, such as non-fungible tokens (NFTs), create opportunities for money laundering in much the same way criminals already exploit art, real estate, or precious metals markets to conceal or transfer illicit wealth.[26]

BITFINEX

The Bitfinex case is an example of the Department's commitment to preventing digital currency heists from undermining confidence in cryptocurrency.

On February 8, 2022, the Department announced the arrest of Ilya Lichtenstein and his wife, Heather Morgan, for an alleged conspiracy to launder cryptocurrency (119,754 bitcoins, or approximately $4.5 billion at the time of the arrest) that was stolen during the 2016 hack of Bitfinex, a virtual currency exchange.[27] So far, law enforcement has seized over $3.6 billion (valued at the time of seizure) of the stolen cryptocurrency. Lichtenstein and Morgan allegedly employed numerous sophisticated laundering techniques, such as using fictitious identities to set up online accounts, using computer programs to automate transactions, depositing the stolen funds into accounts at different exchanges and markets and then withdrawing them to break up the fund flow, converting bitcoin to other forms of virtual currency (including AECs) to engage in "chain-hopping," and using United States-based business accounts to legitimize their banking activity.

Several domestic law enforcement agencies cooperated on the Bitfinex case, including the Internal Revenue Service-Criminal Investigation (IRS-CI); the FBI; and Immigration and Customs Enforcement, Homeland Security Investigations (HSI).

HELIX

The Helix case illustrates the rise of cryptocurrency "mixers" or "tumblers" that pool together funds from multiple sources and can serve to conceal the true ownership or location of criminal proceeds.

On February 13, 2020, the Department announced the indictment and arrest of Larry Harmon, the administrator of Helix, a darknet cryptocurrency laundering service. As alleged in court documents, Helix allowed customers to send bitcoin to designated recipients in a manner designed to conceal the source or owner of the bitcoin. Helix was linked to and associated with "Grams," a darknet search engine also run by Harmon. Helix partnered with several darknet markets selling drugs and other illegal goods and services, including AlphaBay, Evolution, and Cloud 9, to provide bitcoin money laundering services for market customers. Helix was operational from 2014 to 2017. During that time period, Helix was responsible for moving more than 350,000 bitcoins (valued at more than $300 million at the time of the transactions) on behalf of customers, with the largest volume associated with darknet markets. On August 18, 2021, Harmon pleaded guilty to money laundering conspiracy arising out of his operation of Helix.[28]

This case was investigated by IRS-CI and the FBI, with assistance from the Department of State's Diplomatic Security Service. On the same day the Helix administrator was arrested

in the United States, the Belize Ministry of the Attorney General and Belize National Police Department, working in coordination with U.S. authorities, executed a search of the administrator's property in Belize.[29]

Helix was also the subject of a parallel civil enforcement action by the Financial Crimes Enforcement Network (FinCEN). On October 9, 2020, FinCEN announced that it assessed a $60 million civil penalty against Harmon for violations of the BSA, including operating an unregistered MSB, failing to implement and maintain an effective AML program, and failing to report suspicious activities. Helix was subject to the BSA because it operated as an exchanger of convertible virtual currencies by accepting and transmitting bitcoin through a variety of means.[30]

3. Crimes Involving or Undermining the Digital Assets Ecosystem

Growing interest in digital assets has created significant market opportunities, but also opportunities for unscrupulous actors to engage in a variety of criminal activities affecting the marketplace. As the digital assets ecosystem continues to grow and diversify, criminal threats targeting that ecosystem continue apace—including theft, fraud, and technology-specific crimes such as cryptojacking (the unauthorized use of someone else's computing resources to mine cryptocurrency).

Theft of digital assets remains an area of substantial concern. According to one estimate from a blockchain analysis company, more than $3.2 billion in cryptocurrency was stolen from individuals and services in 2021.[31] This represents a significant year-on-year increase, almost six times the amount stolen in 2020, driven in large part by victimization of DeFi platforms, whose open-source architecture makes it easier for attackers to identify security vulnerabilities or exploit flaws in smart contract code.[32] One of the largest cryptocurrency heists to date occurred in March 2022, when, as noted above, the Lazarus Group stole more than $600 million in cryptocurrency from an online gaming platform by exploiting a security flaw in the platform's bridge software, which allows cryptocurrencies to move across different blockchains.

Fraud accounted for another $7.7 billion in losses in 2020, according to the same blockchain analysis company.[33] Many of these losses come from "romance" scams and confidence frauds in which victims are tricked into transferring assets—including cryptocurrency and other assets—to fraudsters or entities under their control. According to data collected by the Federal Trade Commission (FTC), the largest reported losses to romance scams during 2021 were paid in cryptocurrency, totaling $139 million, with a median individual cryptocurrency loss of $9,770.[34] Other losses arise from Ponzi schemes, frauds involving initial coin offerings (ICOs), and "rug pull" schemes in which fraudsters promote new cryptocurrency projects to attract investors, only to steal investors' money and disappear. The Consumer Financial Protection Bureau (CFPB) published 2,404 cryptocurrency-related consumer complaints in its Consumer Complaint Database during 2021, and more than 1,000 cryptocurrency-related complaints during 2022 year-to-date.[35] The CFPB has also received hundreds of servicemember complaints involving cryptocurrency assets or exchanges in the last 12 months, approximately one-third of which concerned frauds or scams.

B. The Growth of Decentralized Finance

Since the publication of the *Cryptocurrency Enforcement Framework* in 2020, the digital assets space has seen dynamic growth in DeFi and the development and popularization of NFTs. These emerging categories of digital assets raise distinct risks for criminal exploitation.

1. Decentralized Finance (DeFi)

DeFi platforms raise novel fraud, consumer and investor protection, and market integrity issues. There is currently "no generally accepted definition of 'DeFi,' or what makes a product, service, arrangement or activity 'decentralized.'"[36] But the term broadly refers to digital asset protocols and platforms that allow for some form of automated peer-to-peer transactions, often through the use of smart contracts based on blockchain technology. Frequently, DeFi platforms purport to run autonomously without the support of a central company, group, or person, relying instead on distributed governance to allow users to make decisions collectively—although some DeFi platforms are decentralized more in name than in fact. DeFi services may include lending, borrowing, purchasing, or trading digital assets, including assets that function as financial products like securities, insurance, or derivatives. DeFi platforms are open for anyone to use and are marketed as an alternative both to traditional financial intermediaries like banks or brokerages, as well as to VASPs that operate as exchanges.[37]

While the transparency of DeFi platforms—typically based on smart contracts and open-source code—is one of their primary features, such transparency also allows malicious actors to identify and exploit vulnerabilities, leading to victim losses and undeniable social harm. Depending on the particular factual circumstances, however, such code exploits may not always map neatly onto the elements of the criminal statutes used most often in fraud or computer intrusion cases, especially in instances where the code itself allows for the exploitation to take place.

DeFi platforms may also raise a host of consumer and investor protection and market integrity concerns of the kind typically subject to state and federal regulation. DeFi platforms offering financial products or services may fall under the jurisdiction of Treasury, the Commodity Futures Trading Commission (CFTC), and/or the Securities and Exchange Commission (SEC), among others.[38] However, because it can be difficult to identify a single person or entity who operates a DeFi platform, enforcing applicable statutory and regulatory obligations can be challenging.

The open-ended nature of DeFi platforms, which are accessible to users worldwide for pseudonymous, one-off transactions, and their ability to execute large, immediate, and automated financial transactions, create substantial money laundering risk. Criminal elements can exploit even well-intentioned DeFi projects if there are insufficient controls to detect and prevent transactions involving funds derived from illegal activity or intended to facilitate criminal activity. And several DeFi projects have affirmatively touted the lack of money laundering controls as one of the primary goals of decentralization. For instance, one cryptocurrency exchange announced in 2021 that it would transition from a traditional corporate structure into a decentralized autonomous organization (DAO) for the stated purpose of ceasing to collect KYC information.[39] Similarly, a founder of an Ethereum-based mixing service purportedly organized it as a DAO to provide automated mixing services.[40] Such examples underscore the need for robust efforts to prevent DeFi from becoming a haven for terrorists, money launderers, and other criminals.

2. Non-Fungible Tokens (NFTs)

NFTs are digital assets, often associated in recent years with a piece of digital artwork, with a unique identifier, as opposed to units of digital currencies that are meant to be interchangeable.[41] The design features of NFTs facilitate their use as certificates of ownership applicable to a wide range of digital and physical assets such as artwork and collectibles.[42] NFTs are frequently built on blockchains like Ethereum or Solana, and are bought and sold on specialized online marketplaces.[43] NFTs are vulnerable to many of the same risks as other digital assets. NFT marketplaces can be hacked and NFTs can be stolen.[44] Unscrupulous promotors can engage in market manipulation, insider trading, and fraudulent schemes.[45] As high-value goods designed to be traded on an anonymous or pseudonymous basis, NFTs are potential vehicles for money laundering or tax evasion schemes.[46] Therefore, there is ample room for law enforcement and regulatory oversight to combat theft and other illegal activity, police market manipulation, and ensure consumer, investor, and market protection in the rapidly changing NFT marketplace.

INSIDER TRADING AND DIGITAL ASSETS

On June 1, 2022, the Department announced an indictment charging Nathaniel Chastain, a former product manager at OpenSea, the largest online marketplace for the purchase and sale of NFTs, with wire fraud and money laundering.[47] Starting around May 2021, OpenSea began to display certain NFTs on its homepage; the featured NFTs changed several times a week. Upon being featured on OpenSea's homepage, an NFT, and other NFTs made by the same NFT creator, often increased substantially in value. Chastain was responsible for selecting the NFTs that would be featured on OpenSea's homepage and therefore knew which NFTs would be featured before this information was available to members of the public. From June 2021 to September 2021, Chastain allegedly used his advance knowledge of OpenSea's confidential business information to buy dozens of NFTs, or other NFTs by the same creator, shortly before those NFTs were featured, and later sold those NFTs at a profit. To conceal the fraud, Chastain conducted these purchases and sales using anonymous digital currency wallets and anonymous OpenSea accounts.

Additionally, on July 21, 2022, the Department unsealed an indictment charging three individuals with wire fraud conspiracy and wire fraud in connection with a scheme to commit insider trading in cryptocurrency assets by using confidential information about which crypto assets were scheduled to be listed on Coinbase Global Inc.'s exchanges.[48] These Coinbase listings typically caused the value of the newly listed assets to increase. The indictment alleges that, on at least 14 occasions between June 2021 and April 2022, Ishan Wahi, a Coinbase product manager, tipped either his brother or friend and associate to forthcoming listings so that those two individuals—charged as Wahi's co-defendants—could, prior to Coinbase's public listings, place profitable trades in the identified crypto assets. To conceal their identities, these co-defendants used accounts at centralized exchanges held in the names of others, and transferred digital assets, including the proceeds of their scheme, through multiple anonymous Ethereum wallets. The two charged recipients of the confidential information collectively generated realized and unrealized gains totaling approximately $1.5 million. After Coinbase announced publicly that it had begun investigating the trading activity, Wahi attempted to flee the United States by purchasing a one-way ticket to India, but he was stopped by law enforcement before boarding his flight.

III. THE ROLE OF LAW ENFORCEMENT AGENCIES, FINANCIAL REGULATORS, AND PRIVATE-SECTOR COOPERATION IN IDENTIFYING AND INVESTIGATING POTENTIAL CRIMINAL ACTIVITY RELATED TO DIGITAL ASSETS

The Department's *Cryptocurrency Enforcement Framework* chronicled the principal legal tools available to investigators and prosecutors pursuing criminals who exploit cryptocurrencies and other digital assets, as well as the important role that U.S. regulatory agencies play in safeguarding the marketplace for digital assets. As explained below, the Department, its law enforcement partners, and financial regulators have enhanced their efforts in the digital assets space since 2020, including through efforts to develop and consolidate subject-matter expertise and benefit from engagement with the private sector.

A. Law Enforcement Efforts and Initiatives

U.S. law enforcement agencies and financial regulators have played a leading role in efforts to combat the illicit use of digital assets, deprive offenders of their ill-gotten gains, and protect consumers from fraud in and manipulation of the digital assets marketplace. As described below, multiple agencies have stepped up their efforts as the use of digital assets has grown in recent years, including by developing and deploying subject-matter expertise, and by conducting domestic and international trainings to help law enforcement and regulatory partners address the risks posed by illicit uses of digital assets.

1. Department of Justice (Criminal and National Security Divisions, FBI, DEA, and U.S. Marshals Service)

The Department has long been at the forefront of efforts to detect, prosecute, and otherwise disrupt criminal activity related to digital assets. Even before the cryptocurrency that some have called "digital gold" (bitcoin) existed, the Department prosecuted the operators of a company whose digital currency (E-Gold) had become a preferred method of online payment for scammers, distributors of child pornography, identity thieves, and other criminals looking to launder money.[49] In the ensuing years, the Department worked with domestic and international partners to shut down Liberty Reserve, at the time one of the world's largest digital-currency companies, and successfully prosecuted several of its principals for running a multi-billion dollar money-laundering scheme.[50] As bitcoin became a preferred payment method in darknet markets, the Department seized the Silk Road marketplace—which accepted payment only in bitcoin—and prosecuted its creator and administrator for conspiring to engage in narcotics trafficking, computer hacking, and money laundering, among other crimes.[51]

The Department has since channeled the expertise developed by its agents, analysts,

prosecutors, and other attorneys to create resources that facilitate cryptocurrency-related investigations nationwide. In 2018, the Criminal Division's Money Laundering and Asset Recovery Section (MLARS) established the Digital Currency Initiative to focus on providing support and guidance to investigators, prosecutors, and other government agencies on cryptocurrency prosecutions and forfeitures.[52] That same year, the Attorney General's Cyber-Digital Task Force released a report that described the Department's emerging practices in tracing, seizing, and liquidating one class of digital assets (virtual currencies), and noted the need to "continue evaluating the emerging threats posed by rapidly developing cryptocurrencies that malicious cyber actors often use," among other things.[53] And in 2020, the Cyber-Digital Task Force published the *Cryptocurrency Enforcement Framework*, which described the legal tools available to successfully prosecute illicit use of cryptocurrencies; profiled the roles and responsibilities of the Department's key government partners in the digital assets space; and noted strategies for addressing emerging threats to the safety and effective operation of the cryptocurrency marketplace.[54]

The Department has redoubled its efforts since the publication of the *Cryptocurrency Enforcement Framework*. In 2021, the Department announced the formation of the NCET to identify, investigate, support, and pursue investigations and prosecutions of criminal misuses of digital assets, with a particular focus on crimes committed by exchanges, mixing and tumbling services, and money laundering infrastructure actors. The NCET is currently composed of over twenty federal prosecutors, investigators, and support staff, including experts detailed from MLARS, CCIPS, U.S. Attorneys' Offices, and the FBI, with additional personnel expected by the end of 2022 from financial regulators. The NCET sets strategic priorities regarding digital asset technologies, identifies areas for increased investigative and prosecutorial focus, tackles issues arising from the application of existing law to novel uses of digital assets, and leads the Department's efforts to coordinate with domestic and international law enforcement partners, regulatory agencies, and private industry to combat the criminal use of digital assets. It also assists in tracing and recovering digital assets, including cryptocurrency payments to ransomware groups, and builds upon and strengthens the capacity of the Department and its partners to dismantle entities that enable criminal actors to flourish and profit from abusing digital asset platforms.

As part of these efforts, NCET members are involved in a variety of cases across the Department, including by leading key digital assets-related investigations and prosecutions (including Hydra, Bitfinex, Helix, BitMEX, and others); participating in significant active litigation regarding legal issues pertaining to digital assets; and providing assistance to others who are tackling cutting-edge cases in the area (including the insider trading cases involving OpenSea and Coinbase). In the past six months, the NCET has provided over 30 trainings for members of federal, state, and foreign law enforcement and judiciaries from Europe, Asia, Africa, the Middle East, and North and South America; and has participated in a variety of different forums and bilateral meetings related to digital assets and cybercrime with foreign partners across six continents, including with G7 partners and at Europol. In addition, the NCET works closely with its domestic law enforcement partners, including experts from the FBI, DEA, IRS-CI, HSI, and the U.S. Secret Service (USSS), and

its regulatory partners, not only on individual investigations but also to set strategic priorities for enforcement and stay apprised of emerging uses of digital asset technologies. Many of these agencies have built or expanded teams focused on digital assets issues, as discussed further in the sections below. The NCET has also consulted with a variety of public and private-sector stakeholders regarding legislative, regulatory, and policy innovations in the digital assets space, and has met with various members of private industry on ways to work together on combating the criminal misuse of digital assets.

On the international front, the NCET is part of the Department's International Virtual Currency Initiative, which was established to focus on strengthening international law enforcement efforts to combat the illicit use of digital assets.[55] The Initiative consists of four primary lines of effort. First, the Criminal Division—in partnership with the Department of State—is working to strengthen international cooperation and capacity with respect to the illicit use of cryptocurrency. Specific efforts on that front include the establishment of regional law enforcement cryptocurrency working groups with select foreign partners, as discussed further in the *International Law Enforcement Cooperation Report*. Second, Resident Legal Advisors funded by the Department of State's Counterterrorism Bureau are increasing their focus on the use of virtual currencies to fund terrorist organizations. Third, the Department is working closely with Treasury, the Department of State, and international partners to promote the implementation of global AML/CFT standards for virtual assets and VASPs, including through work at the FATF through the U.S. delegation led by Treasury's Office of Terrorist Financing and Financial Crimes. Fourth, the NCET is working to identify and recommend additional measures that can be taken to strengthen international law enforcement cooperation to address and combat criminal activity related to digital assets, building upon those recommendations set forth in the June 2022 *International Law Enforcement Cooperation Report*. In doing so, the NCET will coordinate with components across the Department, building on the lessons learned across these lines of effort and the Department's experience in investigating misuse of digital assets here and abroad, as well as with the Department's key domestic partners.

With regard to the FBI, the rise of criminal misuse of digital assets has led to increased prioritization and resources devoted to digital assets-related investigations. As of July 2022, the FBI identified a digital assets nexus in more than 1,100 separate investigations across more than 100 distinct investigative program categories, from violent crimes and gangs to weapons of mass destruction to public corruption and terrorism. Since FY2014, the FBI has seized approximately $427 million in virtual assets (valued at the time of seizure). The FBI has also worked joint investigations supporting partner agencies that resulted in the seizure of billions of dollars in virtual assets. And in February 2022, the FBI formed the Virtual Assets Unit (VAU), a specialized team dedicated to investigating cryptocurrency-related crimes. As the Deputy Attorney General observed in her remarks at the annual Munich Cyber Security Conference in February 2022,[56] the VAU centralizes the FBI's cryptocurrency expertise into one nerve center, providing technological equipment, blockchain analysis and digital asset seizure training, and other sophisticated crypto training for FBI personnel. The VAU is helping to enhance the FBI's ongoing efforts in the digital

assets arena, including its development of a full-scale digital asset training curriculum—the first of its kind—to equip FBI employees, prosecutors, and international partners to identify digital assets in their cases, exploit the resulting financial intelligence, investigate the criminal activity, seize and forfeit digital assets, and build a more accurate threat picture. The FBI has already used this curriculum to train thousands of FBI employees and partners around the globe.[57]

DIGITAL ASSET COORDINATORS NETWORK

To ensure that the Department continues to meet the challenge posed by the illicit use of digital assets, the Criminal Division recently launched the nationwide Digital Asset Coordinators (DAC) Network. The DAC Network is composed of designated federal prosecutors from U.S. Attorneys' Offices nationwide and the Department's litigating components. Led by the NCET, and in close coordination with CCIPS and the MLARS Digital Currency Initiative, the DAC Network serves as a forum for prosecutors to obtain and disseminate training, technical expertise, and guidance about the investigation and prosecution of digital asset crimes. Each DAC acts as their district's or litigating component's subject-matter expert on digital assets, serving as a first-line source of information and guidance about legal and technical matters related to these technologies.

As members of the DAC Network, prosecutors will learn about the application of existing authorities and laws to digital assets and best practices for investigating digital assets-related crimes, including for drafting search and seizure warrants, restraining orders, criminal and civil forfeiture actions, indictments, and other pleadings. The DAC Network will also serve as a source of information and discussion addressing new digital asset forms, such as DeFi, smart contracts, and token-based platforms. In addition, the DAC Network will raise awareness of the unique international considerations of the crypto ecosystem, including the benefits of leveraging foreign relationships and the challenges of cross-border digital asset investigations.

The DAC Network will be a crucial part of the Department's efforts to continue to address the ever-evolving challenges posed by the illicit use of digital assets, by ensuring that prosecutors receive training, technical expertise, investigative resources, and direct legal guidance for investigations and prosecutions in this area. The DAC Network is modeled on the success of two previously established coordinator programs: the Computer Hacking and Intellectual Property (CHIP) Network and the National Security Cyber Specialist (NSCS) Network. The Criminal Division established the CHIP coordinator program in 1995 to ensure that each U.S. Attorney's Office and litigating division has at least one prosecutor who is specially trained on cyber threats, electronic evidence collection, and technological trends that criminals exploit.[58] The National Security Division similarly launched the NSCS Network in 2012 to equip U.S. Attorneys' Offices "around the Nation with prosecutors trained on national security cyber threats, such as nation-state cyber espionage."[59]

The foregoing Criminal Division sections are not the only Department components investigating and prosecuting crimes related to digital assets. Rather, several other Department components have assigned individuals with experience in digital asset investigations to handle such matters, or serve as points of contact, when they arise. For example, the Market Integrity and Major Frauds Unit within the Criminal Division's Fraud Section has attorneys who specialize in digital asset investigations and who have played a central role in multiple recent investigations that culminated in charges, including the series of prosecutions described below. Likewise, several of the prosecutors who handle cyber investigations within the National Security Division's (NSD) Counterintelligence and Export Control Section are specifically tasked with handling complicated cryptocurrency issues in the national security context, such as the seizure of digital assets from DPRK ransomware actors,[60] and the recovery of the Colonial Pipeline ransomware payment.[61] NSD's Counterterrorism Section has also assigned some of its trial attorneys to track that Section's encounters with cryptocurrency-related issues and to serve as liaisons with other Department components and other agencies, where necessary. Finally, the U.S. Attorneys' Offices from across the country investigate and prosecute a wide array of different crimes involving digital assets, often in conjunction with other Department components.

RECENT CRYPTOCURRENCY FRAUD PROSECUTIONS

On June 30, 2022, the Department announced charges against six individuals in four cases involving over $100 million in intended losses from cryptocurrency fraud offenses.[62] These charges were brought in conjunction with law enforcement and regulatory partners, and one of them has already resulted in a guilty plea.

In the first case, which involved NFTs, a Vietnamese national was charged with conspiracy to commit wire fraud and conspiracy to commit international money laundering. As alleged in the indictment, the defendant was involved in an NFT-investment project known as the Baller Ape Club, which purportedly sold NFTs in the form of various cartoon figures, including the figure of an ape. Soon after the Baller Ape Club publicly sold its first NFTs, the defendant and his co-conspirators allegedly engaged in a "rug pull," in which they ended the purported investment project, deleted its website, and then attempted to launder approximately $2.6 million of investors' money.

In the second case, three defendants—two from Brazil and one from Florida—were charged with wire and securities fraud conspiracies, with two of the defendants additionally facing a charge of conspiracy to commit international money laundering. The charges arose from a global cryptocurrency-based Ponzi scheme that generated approximately $100 million from investors. The indictment alleges that the defendants fraudulently promoted EmpiresX, a cryptocurrency investment platform and unregistered securities offering, by making numerous misrepresentations regarding, among other things, a purported proprietary trading bot, and fraudulently guaranteeing returns to investors and prospective investors in EmpiresX.[63]

The indictment in the third case alleges that the owner of Circle Society, a cryptocurrency investment platform, used the platform to solicit investors to participate in an unregistered commodity pool, which is a fund that combines investors' contributions to trade on the futures and commodity markets. As alleged in the indictment, the defendant falsely represented that he traded investors' funds to earn profits using a trading bot that could execute over 17,000 transactions per hour on various cryptocurrency exchanges and generate between 500% to 600% returns on the amount invested. In total, the defendant fraudulently raised approximately $12 million from investors.[64]

The defendant in the fourth case, Michael Alan Stollery, was the CEO and founder of Titanium Blockchain Infrastructure Services (TBIS), a purported cryptocurrency investment platform. On July 22, 2022, Stollery pleaded guilty to one count of securities fraud for his role in a cryptocurrency fraud scheme involving TBIS's ICO, which raised approximately $21 million from investors in the United States and other countries.[65] Stollery admitted as part of his plea that, to entice investors, he falsified aspects of TBIS's white papers (a document for prospective investors that typically explains how the technology underlying the cryptocurrency works and the purpose of the cryptocurrency project), planted fake testimonials on TBIS's website, and fabricated purported business relationships with the U.S. Federal Reserve Board and dozens of prominent companies to create the appearance of legitimacy. Stollery's sentencing is currently scheduled for November 2022.

Also housed within the Department, the DEA is a key player in narcotics investigations involving the use of cryptocurrency on darknet markets and by transnational criminal organizations. DEA's Special Operations Division serves as a critical coordination and deconfliction center for drug trafficking cases, including those matters involving cryptocurrency. In addition, DEA's Cyber Support Section provides subject-matter expertise with respect to investigative tactics, techniques, and tools related to cryptocurrency. DEA is prioritizing the development of deep technical expertise, robust capabilities, and strong international and domestic partnerships to combat the use of cryptocurrency to facilitate drug trafficking within the United States and transnationally.

Finally, as the primary custodian of seized cryptocurrency for the Department and HSI, the United States Marshals Service provides a variety of services to manage and dispose of seized digital assets, including by liquidating them so that funds may be returned to victims, where appropriate, or otherwise used as part of the Department's Asset Forfeiture Program. The Marshals Service has a team of federal employees and contractors who are dedicated to the management and disposal of cryptocurrency. Those team members have diverse backgrounds in finance, asset management, policy development, and forfeiture. In addition, the Marshals Service plans to award a new competitive national contract for custodial and disposal services related to virtual currency in FY2023, which

will enable the Marshals Service to use industry expertise to manage evolving types of virtual currency efficiently and securely while avoiding significant expenditure on technology and staff.

2. Department of Homeland Security (HSI and USSS)

Two components of the Department of Homeland Security—HSI and the Secret Service—have played key roles in some of the most significant digital assets-related investigations, from the pre-bitcoin E-Gold prosecution, to the recent takedown of the Hydra darknet marketplace.

HSI works to combat the criminal exploitation of digital currencies through multiple units. Since FY2014, HSI has seized approximately $138 million in virtual assets (valued at the time of seizure). Currently, HSI has more than 500 active investigations that involve digital assets in some manner.

HSI has developed a robust training and outreach program through coordination of three of its units that focus on investigations involving digital assets: the Cyber Financial Section of the Financial Crimes Unit (FCU), which is charged with the oversight of all HSI financial investigations; the Cyber Crimes Center (C3); and the Asset Forfeiture Unit (AFU). This training program is intended to equip HSI field agents and other investigative personnel with up-to-date information and techniques to (1) identify digital assets that are proceeds or used in furtherance of criminal activities, (2) identify and unmask financial transactions involving these digital assets, and (3) seize and forfeit these assets to help disrupt and dismantle criminal organizations and deter criminal activity.[66] The FCU, C3, and AFU work diligently to train not only HSI special agents, but also state and local law enforcement partners around the United States and internationally. In FY2022 to date, HSI has conducted outreach or training to approximately 474 state and local law enforcement officers.

For its part, the USSS investigates a variety of cyber-related criminal activity, including the illicit use of digital assets, through its global network of 44 Cyber Fraud Task Forces. From January 2015 through July 2022, the Secret Service investigated more than 302 cases involving digital assets, resulting in 535 seizures with an appraised value of over $113.5 million (as measured at the date of the seizure).

The Secret Service also dedicates substantial resources to training law enforcement partners both internationally—as described in the *International Law Enforcement Cooperation Report*—and domestically. On the domestic front, at its National Computer Forensics Institute (NCFI), the Secret Service trains state, local, tribal, and territorial (SLTT) law enforcement personnel on preventing, mitigating, and responding to cyber attacks, including those associated with the illicit use of digital assets. The NCFI provides digital currency training for USSS Special Agent trainees as part of their initial investigative training, as well as a digital currency course for SLTT partners.

Additionally, in February 2022, the USSS announced the launch of its online Awareness Hub on cryptocurrency and other digital assets,[67] which aims to provide the public with information on digital asset security and features the agency's latest efforts in combating illicit use of digital assets.[68]

3. Department of the Treasury (IRS-CI)

Leveraging years of tracing traditional money flows, IRS-CI leads the IRS's investigations of criminal activity related to cryptocurrency and other digital assets. IRS-CI agents have either led or contributed to cryptocurrency-focused investigations in which the cryptocurrency facilitated tax violations, pyramid schemes, investment fraud schemes, cryptocurrency exchanges, darknet mixers, darknet markets, terrorist organizations, DPRK hacking and fundraising campaigns, and a child exploitation darknet site. As reflected in the wide range of subjects involved in those investigations, IRS-CI focuses its efforts not on the underlying crime but on the financial aspects of a crime.

BITQYCK

In March 2022, Bruce Bise and Samuel Mendez were sentenced to a combined eight years of imprisonment for tax evasion stemming from a fraudulent cryptocurrency investment scheme.[69] Bise and Mendez were the founders of Bitqyck, whose cryptocurrency (Bitqy) they promoted as a way for individuals who had missed out on bitcoin's appreciation. Among other things, materials posted on Bitqyck's website promised investors that each Bitqy token purchased in Bitqyck's 2016 ICO came with a fractional share of Bitqyck common stock. Bise and Mendez, however, never distributed shares to token holders or embedded the shares within the Ethereum smart contract. Instead, the only Bitqyck common stock issued went to Bise and Mendez, who collectively owned 100% of the company's common stock.

Bise and Mendez profited from Bitqyck by diverting income from the company for their personal use at their shareholders' expense. From 2016 to 2018, Bise and Mendez took in more than $4 million each. Although taxpayers transacting in virtual currency are required by law to report those transactions on their tax returns, Bise and Mendez both underreported their income to the IRS, resulting in a tax loss of more than $300,000 for each of them for 2016 and 2017. In 2018, Bitqyck failed to file any corporate tax returns at all despite netting more than $3.5 million from investors. The total tax loss to the United States government between Bise and Mendez was more than $1.6 million dollars. The case was investigated by IRS-CI.

The guilty pleas and criminal sentences followed a settlement agreement with the SEC, in which Bitqyck agreed to pay an $8.3 million penalty to resolve claims that it defrauded investors and operated an unregistered digital asset exchange, and Bise and Mendez each agreed to pay disgorgement and penalties of more than $850,000.[70]

As part of its efforts, IRS-CI is establishing an Advanced Collaboration and Data Center (ACDC) in Northern Virginia to improve investigations into the use of digital currencies in illicit activities, including unauthorized computer intrusions, human trafficking, and drug trafficking. The ACDC will be a mission-centric hub for specialized personnel, data, and technology within the IRS, the Treasury Department as a whole, and partnering agencies, with the objective of providing both a common focus area and a value-added resource.[71]

Apart from its investigative functions, IRS-CI has organized and participated in several engagements to share best practices with, and build the capacity of, international partners. Those efforts—along with the Department's training and capacity-building efforts—are more fully described in Annex C to the *International Law Enforcement Cooperation Report*.

B. Department Coordination With Regulatory Agencies

For more than a century, the United States has developed a robust legal and regulatory framework for its financial system, which protects and promotes the national economy and the national interest, and which has continuously been updated and revised to address new threats. Regulatory agencies have continued to take proactive steps in recent years in response to the rise of digital assets. It is a critical policy goal of the United States to ensure that digital assets do not undermine existing financial regulations, and to provide strong incentives for institutions and exchanges to operate within the existing digital assets-related regulatory framework.

Regulatory agencies play a crucial, multifaceted role in meeting that policy goal. They provide guidance to regulated entities about how existing statutes and regulations apply to digital asset technologies, monitor compliance with regulations, and bring enforcement actions, among other things. The Department's criminal prosecutions build on this work and play an important complementary role by penalizing the worst offenders who flout their regulatory obligations and by deterring others from operating outside of the applicable regulatory framework. This section discusses some of the key regulations that apply to digital assets and the coordinated work of federal regulatory agencies and the Department of Justice in ensuring that those regulations are followed.

1. Treasury (FinCEN)

One key component of the digital assets-related legal and regulatory framework is the BSA and the regulations issued thereunder, including rules requiring financial institutions to have AML/CFT programs. Among other things, these rules aim to prevent criminals from using the financial system to commit fraud, engage in money laundering, or finance terrorist activity. The Department of the Treasury's FinCEN has primary responsibility for administering the BSA and for implementing its regulations.[72]

FinCEN guidance has long stated that the BSA covers "value that substitutes for currency" (*i.e.*, virtual currency) as it relates to money transmission and money transmitters.[73] A person, regardless of their location, doing business as a money transmitter wholly or in substantial part in the United States, including through virtual currency or other digital asset transactions, must register as a MSB and comply with AML/CFT requirements.[74] In 2019, FinCEN published additional guidance focusing on virtual currency-related businesses.[75]

Among the AML/CFT obligations that attach to persons acting as money transmitters are the requirements to monitor for suspicious transactions and file suspicious activity reports (SARs) with FinCEN. SARs serve a critical role for law enforcement and financial regulators, generating important information about potential criminal activity that can prompt or assist an investigation. A business that operates as a money transmitter without a required state or federal registration can also be criminally prosecuted under 18 U.S.C. § 1960.

An important recent example of how FinCEN and the Department's efforts can complement each other is the Bitcoin Mercantile Exchange (BitMEX) investigation, in which FinCEN and the CFTC brought enforcement actions that proceeded in parallel with a criminal prosecution of four BitMEX executives. The BitMEX case is discussed later in this Report.

2. Treasury (OFAC)

Financial regulations also play a key role in protecting national security, including through the designation of certain individuals and entities for sanctions based on a determination that they pose a threat to the national security, foreign policy, or economy of the United States. The Department of the Treasury's Office of Foreign Assets Control (OFAC) administers sanctions, monitors compliance with these sanctions, and conducts civil investigations into apparent violations of sanctions regulations. OFAC has recognized that digital assets can be used by individuals and entities who seek to violate or evade U.S. sanctions. As with BSA compliance, criminal prosecution plays an important role in complementing OFAC's regulatory oversight.

Since 2018, OFAC has been active in the digital assets area, imposing sanctions on perpetrators of ransomware attacks, who often make ransom demands in cryptocurrency; entities that facilitate the digital ransom payments; and more recently, "nested" cryptocurrency exchanges,[76] a darknet market,[77] and mixers that were used by a variety of illicit actors, including the DPRK to support its malicious cyber activities and laundering of stolen virtual currency. Specifically, in May 2022, OFAC issued sanctions for the first time against a virtual currency mixer, Blender.io, which the DPRK used to support its malicious cyber activities and associated money laundering.[78] Approximately six weeks before OFAC's actions, Lazarus Group, the DPRK state-sponsored cyber hacking group, carried out the largest virtual currency heist to date—worth almost $620 million at the time—from a blockchain project linked to the online game Axie Infinity. Blender.io, a mixer that obfuscates transactions on the Bitcoin blockchain, was used in processing more than $20.5 million of the illicit proceeds. And in August 2022, OFAC issued sanctions against an additional virtual currency mixer, Tornado Cash, which had been used to launder more than $7 billion worth of virtual currency since its creation in 2019, including over $455 million stolen by the Lazarus Group.[79] U.S. persons are prohibited from engaging in any transactions or dealings with sanctioned individuals or entities and must block any of their assets that are in their possession or control.

In addition to these sanctions actions, in 2021, OFAC published sanctions compliance guidance for the virtual currency industry.[80] OFAC also issued a ransomware advisory that describes sanctions risks associated with ransomware payments and encourages companies to report attacks to, and cooperate with, law enforcement, and adopt and improve cybersecurity practices.[81]

USE OF ONLINE PAYMENT SYSTEMS TO EVADE SANCTIONS

A recent criminal prosecution illustrates how criminal actors attempt to use online payments in digital assets as a method for evading U.S. sanctions.

In an opinion partially unsealed on May 13, 2022, a magistrate judge in the U.S. District Court for the District of Columbia ruled that the Department demonstrated probable cause in a criminal complaint to obtain an arrest warrant for an unnamed defendant, who is accused of transmitting more than $10 million in bitcoin to a "comprehensively sanctioned" country.[82] According to the criminal complaint, the defendant and others operated an online payments and remittances platform based in the sanctioned country. The defendant registered various domain names for the payment platform, paid for by a company created in the United States, and used a U.S.-based online financial institution account to receive and send thousands of dollars to the sanctioned country for customers of the payments platform. The defendant also opened an account on a U.S.-based virtual currency exchange and purchased bitcoin using fiat currency. These funds were then transferred to an account at an overseas virtual currency exchange, from which customers of the payments platform could access the virtual currency. More than $10 million worth of bitcoin was transferred between the United States and the sanctioned country using this method.

In finding probable cause, the magistrate judge cited OFAC's guidance that "sanctions compliance obligations *apply equally* to transactions involving virtual currencies and those involving traditional fiat currencies."[83] The court noted that OFAC had initiated multiple civil enforcement actions involving the use of virtual assets to violate U.S. sanctions, and explained that "civil liability is not the ceiling" and that individuals and entities that fail "to comply with OFAC's regulations, including as to virtual currency," could be criminally prosecuted as well.[84]

With respect to investigations involving digital assets, OFAC's primary enforcement focus has been on detecting and investigating potential violations of U.S. sanctions by U.S. persons or other persons subject to U.S. jurisdiction, including virtual currency exchanges, wallet software providers, decentralized exchange providers, NFT marketplaces, and other digital assets-related service providers. Since 2020, OFAC has twice entered into settlement agreements with U.S.-based companies in the digital assets space for providing financial services to persons apparently located in sanctioned jurisdictions. In December 2020, OFAC announced a settlement with BitGo, Inc., a technology company based in California. BitGo agreed to remit $98,830 to settle its potential civil liability for 183 apparent violations of multiple sanctions programs.[85] As a result of deficiencies related to BitGo's sanctions compliance procedures, BitGo failed to prevent persons apparently located in the Crimea region of Ukraine, Cuba, Iran, Sudan, and Syria from using its non-custodial secure digital wallet management service. BitGo had reason to know that these users were located in sanctioned jurisdictions based on Internet

Protocol (IP) address data associated with devices used to log in to the BitGo platform. At the time of the transactions, however, BitGo failed to implement controls designed to prevent such users from accessing its services.

In February 2021, OFAC announced a settlement with BitPay, Inc., a private company based in Atlanta, Georgia, that offers a payment processing solution for merchants to accept digital currency as payment for goods and services. BitPay agreed to remit $507,375 to settle its potential civil liability for 2,102 apparent violations of multiple sanctions programs.[86] BitPay allowed persons who appear to have been located in the Crimea region of Ukraine, Cuba, North Korea, Iran, Sudan, and Syria to transact with merchants in the United States and elsewhere using digital currency on BitPay's platform—even though BitPay had location information, including IP addresses and other location data, about those persons prior to effecting the transactions.

To support its investigative efforts, OFAC has also focused on building technical expertise among its enforcement and compliance officers, including through training on the use of blockchain analytics tools. Additionally, OFAC leverages financial and other intelligence information to detect and investigate violations of U.S. sanctions involving digital assets. OFAC also refers potential criminal violations of U.S. sanctions involving digital assets to the Department. OFAC has strong working relationships with the Department and other law enforcement partners, including IRS-CI, which allows all such partners to coordinate investigations, share resources, develop leads, and leverage subject-matter expertise. OFAC also regularly provides training to domestic law enforcement partners on U.S. sanctions, including identifying typologies and fact patterns that may indicate violations of U.S. sanctions using digital assets.

GRIFFITH

The prosecution of Virgil Griffith is an example of the Department's commitment to preventing U.S. persons from assisting sanctions violations through the use of digital assets.

Griffith was a cryptocurrency expert who traveled to the DPRK in April 2019 to provide instructions on how the DPRK could use blockchain and cryptocurrency technology to launder money and evade sanctions.[87] Griffith understood that his audience included individuals who worked for the DPRK government, and answered specific technical questions they had about blockchain and cryptocurrency technologies. He did so knowing that the DPRK could use these services to evade and avoid U.S. sanctions, and to fund its nuclear weapons program and other illicit activities.

On September 27, 2021, Griffith pleaded guilty to conspiracy to violate the International Economic Emergency Powers Act, 50 U.S.C. § 1701 *et seq*. On April 12, 2022, he was sentenced to 63 months' imprisonment.

3. Securities and Exchange Commission (SEC)

The SEC's mission is to protect investors; to maintain fair, orderly, and efficient markets; and to facilitate capital formation. The *Cryptocurrency Enforcement Framework* detailed much of the SEC's critical work in responding to the growth of offers and sales of digital assets, such as ICOs.[88] In 2017, the SEC issued an investigative report cautioning the public that offers and sales of digital assets—including through ICOs—by "virtual" organizations may be subject to the requirements of the federal securities laws, which include registration and disclosure mandates.[89] As the SEC explained, "[w]hether or not a particular transaction involves the offer or sale of a security—regardless of the terminology or technology used—will depend on the facts and circumstances, including the economic realities of the transaction."[90] The term "security" includes an "investment contract," as well as other instruments such as stocks, bonds, and transferable shares.[91] Under the "*Howey* test," derived from the Supreme Court's seminal 1946 decision in *Securities and Exchange Commission v. W. J. Howey Co*., an "investment contract" exists if there is an investment of money in a common enterprise with an expectation of profits derived from the efforts of others.[92]

To date, the SEC has brought more than 100 enforcement actions involving digital assets, including ICOs, unregistered securities exchanges, and DeFi protocols. And courts have recognized that the *Howey* test applies to offerings of digital assets. For example, on September 30, 2020, a federal district court in New York held in *SEC v. Kik Interactive Inc*. that the issuer's offering of the "Kin" token was an investment contract under *Howey*, and therefore an offering of securities.[93] The court went on to find that Kik, the issuer, had violated the federal securities laws when it conducted an unregistered offering that did not qualify for any exemption from registration requirements. In response to Kik's argument that the term "investment contract" was unconstitutionally vague as applied to Kik, the court stated that "*Howey* provides a clearly expressed test for determining what constitutes an investment contract, and an extensive body of case law provides guidance on how to apply that test to a variety of factual scenarios."[94]

The SEC coordinates its oversight of and response to emerging technologies in financial, regulatory, and supervisory systems—including in the area of digital assets—through the Strategic Hub for Innovation and Financial Technology (FinHub).[95] In recent years, the SEC has committed substantial additional resources to monitoring and enforcing the securities laws in the digital asset space. For instance, in February 2022, the SEC charged a crypto asset platform, BlockFi Lending LLC, with failing to register the offers and sales of its retail crypto lending product and with failing to register as an investment company.[96] The SEC's order found that BlockFi unlawfully sold securities through which investors lent crypto assets to BlockFi in exchange for the company's promise to provide a variable monthly interest payment. Without admitting or denying the SEC's findings, BlockFi agreed to pay a $50 million penalty, cease its unregistered offers and sales of the lending product, and attempt to bring its business within the provisions of the Investment Company Act. In parallel actions, BlockFi agreed to pay an additional $50 million in fines to 32 states to settle similar charges.

In August 2021, the SEC charged two individuals and their Cayman Islands company for unregistered sales of more than $30 million

in securities using smart contracts and so-called DeFi technology and for misleading investors concerning the operations and profitability of their business "DeFi Money Market."[97] The SEC's order found that the respondents used smart contracts to sell two types of digital tokens: one that could be purchased using specified digital assets and that paid a given percent interest, and another so-called "governance token" that purportedly gave holders certain voting rights, a share of excess profits and the ability to profit from token resales in the secondary market. The order further found that the respondents misrepresented how the company was operating. The order found that the two types of tokens were offered and sold as securities and that respondents had violated the registration and antifraud provisions of the federal securities laws. Without admitting or denying the findings in the order, the respondents consented to a cease-and-desist order, including disgorgement totaling more than $12 million and penalties of $125,000 for each of the respondents.

BITCONNECT

The BitConnect case is not only an example of the government's commitment to a collaborative multi-agency approach to cryptocurrency crimes, but also a striking reminder that online-based crimes are often derivative of traditional crimes that the Department has targeted for decades.

On February 25, 2022, the Department announced criminal charges against Satishkumar Kurjibhai Kumbhani, an Indian national and the founder of the cryptocurrency company BitConnect.[98] This indictment follows the September 2021 guilty plea by BitConnect's head U.S. promoter, Glenn Arcaro. BitConnect had sought to exploit investor interest in cryptocurrency by fraudulently marketing BitConnect's proprietary coin offering and digital currency exchange as a lucrative investment.[99] BitConnect had, moreover, solicited investors by fraudulently claiming that BitConnect's purported proprietary technology, known as the "BitConnect Trading Bot" and "Volatility Software," were able to generate substantial profits and guaranteed returns. In reality, however, the purported technologies generated no such profits and merely functioned as a cover for BitConnect's criminal schemes. Indeed, BitConnect essentially operated as a textbook Ponzi scheme, with the company paying earlier BitConnect investors with money from later investors. Ultimately, the BitConnect scheme defrauded investors from the United States and abroad of over $2 billion and is the largest cryptocurrency fraud the Department has ever charged criminally.

In a parallel action, the SEC announced civil charges against the masterminds behind BitConnect, including Kumbhani and Arcaro, on September 1, 2021, alleging that they had defrauded retail investors out of $2 billion through a fraudulent and unregistered offering of investments involving digital assets.[100] The SEC's complaint charged Kumbhani and Arcaro with violating the antifraud and registration provisions of federal securities laws, and sought injunctive relief, disgorgement of unlawful profits plus interest, and civil penalties.

On May 3, 2022, the SEC announced that it was nearly doubling the size of the enforcement unit responsible for protecting investors in crypto markets and from cyber-related threats.[101] As announced, the newly renamed and expanded Crypto Assets and Cyber Unit (formerly known as the Cyber Unit) will continue to address cyber-related threats in the nation's markets. It will also leverage the agency's expertise to ensure investors are protected in the crypto markets, with a focus on investigating securities law violations related to crypto asset offerings, crypto asset exchanges, crypto asset lending and staking products, DeFi platforms, NFTs, and stablecoins.

The Department works in parallel with the SEC to enforce the nation's securities laws in the digital asset space. The BitConnect case referenced earlier in this Report is an example of how the Department's law enforcement role and the SEC's civil enforcement role can mutually reinforce each other to protect investors and the integrity of the markets against securities fraud schemes.

4. Commodity Futures Trading Commission (CFTC)

The CFTC has regulatory jurisdiction and enforcement authority over commodity derivatives and transactions that function as derivatives on commodities, as well as fraud and manipulation authority in connection with commodities in interstate commerce. The Commodity Exchange Act (CEA) provides that the CFTC "shall have exclusive jurisdiction" over commodity options, swaps (excluding security-based swaps, which usually fall under SEC jurisdiction), and contracts of sale of a commodity for future delivery (*i.e.*, futures contracts). The CEA also provides that the CFTC may enforce the CEA's prohibitions against fraud and manipulation in connection with "a contract of sale of any commodity in interstate commerce."[102] The CEA defines "commodity" broadly to include a long list of physical goods as well as "all other goods and articles . . . and all services, rights, and interests . . . in which contracts for future delivery are presently or in the future dealt in."[103] Numerous registered entities offer crypto asset-based derivatives, which allows for direct CFTC oversight of certain exchanges and market participants associated with digital asset markets.

Since 2015, the CFTC has brought numerous digital assets-related enforcement actions against entities located in the United States and abroad, and regularly cooperates with domestic and foreign counterparts in connection with related enforcement investigations. The CFTC has asserted jurisdiction over digital asset transactions, including virtual currency transactions in a variety of contexts,[104] beginning in 2015 with an administrative order settling charges against Coinflip, Inc.[105] Multiple federal courts have recognized that cryptocurrencies are commodities under the Commodity Exchange Act.[106] For example, in February 2022, a federal court held that the law was sufficiently clear that a criminal defendant "had adequate notice that cryptocurrencies were commodities within the meaning of the CEA," and denied a motion to dismiss an indictment brought by the Department against executives at the Bitcoin futures exchange BitMEX, a case that is discussed in further detail below.[107]

To date, the CFTC has brought over 50 enforcement actions involving digital assets, including 23 matters filed in fiscal year 2021 against defendant entities located in the United States and abroad. CFTC enforcement actions have included cases charging retail fraud;[108] cases charging unregistered trading platforms

with illegally offering off-exchange trading in derivatives on digital assets;[109] cases charging unregistered futures commission merchants (FCM) with soliciting and accepting orders for derivatives or derivative-like products on digital asset transactions with customers and accepting money or property (or extending credit in lieu thereof) to margin those transactions;[110] cases addressing AML violations; and cases addressing misconduct across a broad range of digital assets, including stablecoins.[111]

For instance, a 2021 CFTC order found that Coinbase recklessly delivered false, misleading, or inaccurate reports concerning transactions in digital assets, including bitcoin, on an electronic trading platform operated by Coinbase.[112] In particular, Coinbase operated at least two trading programs which generated orders that, at times, matched with one another. Coinbase included the transactional information for these transactions, such as price and volume data, on its website and provided that information to reporting services, either directly or through access to its website, resulting in a perceived volume and level of liquidity of digital assets, including bitcoin, on Coinbase's exchange that was false, misleading, or inaccurate.

"Pump and dump" price manipulation on spot exchanges comprises another category of CFTC enforcement action based on spot transactions. In the first such action, titled *CFTC v. McAfee & Watson*, No. 21-cv-1919 (S.D.N.Y.), the defendants secretly accumulated positions in certain cryptocurrencies, including Dogecoin, and then touted the attributes of those assets on social media while at the same time selling off their positions at substantial profits when the prices rose as a result of the defendants' statements.[113]

In some cases, unregistered platforms offering transactions in derivatives on digital assets unlawfully act in more than one unregistered capacity. For example, a 2021 CFTC order found that Payward Ventures, Inc. (d/b/a Kraken) unlawfully offered off-exchange margined retail commodity transactions and also acted as an unregistered FCM by accepting orders for and entering into retail commodity transactions with customers, and accepting money or property (or extending credit in lieu thereof) to margin these transactions.[114]

The CFTC has also addressed misconduct in DeFi markets. For example, a 2022 CFTC order found that Blockratize, Inc. (d/b/a Polymarket) unlawfully offered off-exchange event-based binary options contracts and failed to obtain designation as a designated contract market or register as a swap execution facility in the derivatives (event contract) markets it operated.[115]

The Department works in parallel with the CFTC to enforce the Commodity Exchange Act and other U.S. laws in the digital asset space. The BitMEX case discussed in detail below is an example of how criminal prosecution plays a key role alongside the CFTC's regulatory enforcement.

BITMEX

The Department's recent BitMEX prosecution illustrates the need to prosecute individuals who operate cryptocurrency platforms that fail to comply with the BSA's AML obligations, alongside regulatory actions taken by agencies such as FinCEN and the CFTC.[116]

BitMEX was an online cryptocurrency derivatives exchange created in 2014 that ultimately became the largest cryptocurrency derivatives exchange in the world. It offered futures and other derivative products to customers. Its operations made it a FCM, which is a type of financial institution that is required to register with the CFTC and implement an AML program, including KYC procedures. However, BitMEX did not institute a BSA-compliant AML program and took no steps to verify its customers' identities, allowing individual customers to trade simply by providing an email address.

BitMEX falsely claimed that it did not serve U.S. customers, but in fact it had extensive U.S.-based operations and served thousands of U.S. customers. As a result of its willful failure to implement AML and KYC programs, BitMEX was in effect a money laundering platform. For example, in May 2018, Arthur Hayes, BitMEX's founder and CEO, was notified of allegations that BitMEX was being used to launder the proceeds of a cryptocurrency hack. However, the company took no steps to file a suspicious activity report, as required by law, and filed no suspicious activity reports from September 2015 through September 2020, the charged time period. An analysis by FinCEN concluded that BitMEX conducted at least $209 million worth of transactions with known darknet markets or unregistered MSBs providing mixing services.[117]

The Department obtained an indictment against four executives of BitMEX—the three founders of the company and the company's U.S.-based head of business development—in October 2020. On the same day, the CFTC announced a civil complaint against the company and its three founders, alleging, among other charges, that they were illegally offering derivative-like digital assets to U.S. customers, failed to register as a FCM, and failed to comply with the BSA. In August 2021, the company settled with the CFTC and also settled a regulatory action brought by FinCEN, agreeing to pay a total of a $100 million fine.[118] Additionally, all four defendants in the criminal case entered guilty pleas in 2022, and each of the three founders agreed to pay a $10 million fine.

5. Banking Regulators

Multiple federal banking regulators oversee the safety and soundness of the national banking system, including the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), and the Federal Reserve Board (FRB). These agencies have also taken recent steps to address the potential risks to the banking system posed by cryptocurrencies and other digital assets.

In November 2021, for example, the OCC published Interpretive Letter 1179 to clarify and explain the supervisory process a national bank should undertake to demonstrate, to the satisfaction of the regulator, that it has controls in place to conduct certain cryptocurrency and distributed ledger related activities in a safe and sound manner.[119] And the FDIC recently issued a letter requiring FDIC-supervised banks that intend to engage in, or that are currently engaged in, any activities involving or related to digital assets to notify the FDIC of these activities, to allow the FDIC to provide regulatory feedback.[120] These agencies have also engaged in regulatory enforcement actions in the digital asset space.[121]

6. Consumer Protection Agencies

Federal consumer protection agencies, including the Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB), enforce laws designed to protect consumers from fraud, abuse, and unfair business practices and to ensure a competitive marketplace. They also serve important roles responding to consumer complaints, collecting data and identifying trends, and educating the public about issues relating to digital assets.

The FTC has a broad mandate under Section 5 of the FTC Act[122] to investigate unfair or deceptive acts or practices in or affecting commerce, including those related to digital assets, as well as to enforce other consumer protection statutes and regulations, such as the Electronic Fund Transfer Act,[123] the Equal Credit Opportunity Act,[124] and the Gramm-Leach-Bliley Act.[125] The FTC's enforcement actions relating to cryptocurrency date back to 2014, when the agency halted a multimillion-dollar operation that failed to deliver on its promise to ship bitcoin mining computers to consumers.[126] Since then, in addition to its enforcement efforts, the FTC has engaged with the public through consumer and business education, including by examining and reporting on trends in consumer complaints received through the agency's Consumer Sentinel Network.[127] The agency has also hosted workshops and panels regarding digital assets that included academics, other regulators, and members of the public,[128] and agency staff have conducted trainings for external organizations, including those focused on populations ranging from college students to older adults.

The CFPB is tasked with regulating the offering and provision of consumer financial products and services under the federal consumer financial laws to ensure that the consumer financial markets are fair, transparant, and competitve—and that all consumers have access to those markets.[129] Through the Office of Enforcement, the CFPB enforces compliance with the federal consumer financial laws, including the Truth in Lending Act, the Electronic Fund Transfer Act, the Equal Credit Opportunity Act, and the Dodd-Frank Act's prohibition against unfair, deceptive, or abusive acts or practices.[130] The CFPB engages in consumer education and releases consumer financial protection circulars, which have addressed issues relating to digital assets.[131] It

also operates a consumer complaint database that has seen a rise in complaints about fraud involving digital assets.[132] The CFPB actively reviews these complaints to inform enforcement actions, identify patterns and trends, and share information across agencies when appropriate.

C. Private Sector Partnerships

The scale of the challenge presented by digital assets also requires partnerships between government actors and the private sector, which can enhance the capacity of regulators and law enforcement to quickly and effectively investigate and disrupt criminal activity.

To begin, the private sector plays the first line of defense in detecting and monitoring suspicious activity that takes place through their institutions and on their own platforms. Entities with robust AML/CFT programs and KYC procedures can play a crucial role in helping to mitigate the risks posed by the illicit use of digital assets to their customers and organizations, and to build trust, transparency, and stability in the digital assets markets. Private sector organizations can also be victims of a wide array of digital assets-related crime, ranging from thefts and frauds to attacks, exploits, and hacks. In all these instances, timely sharing of information and cooperation with law enforcement are important not only to protect other companies from future victimization, but also to best position law enforcement to investigate and disrupt the criminal actors. Because criminal actors using these technologies can victimize targets quickly, move funds nearly instananeously across the globe, and take steps to attempt to cover their tracks, investigations involving digital assets must be fast-moving. Private sector cooperation with law enforcement is therefore critical to efforts to investigate and disrupt the illicit use of digital assets, including through sharing information about criminal attacks; seizing online infrastructure used in these attacks; apprehending and prosecuting those responsible; and seizing digital assets to be returned to victims, where appropriate.

Private sector actors also play a role in providing services to the government that may be difficult for the government to replicate at similar efficiency, such as blockchain analytics tools, which serve as a key component of almost any cryptocurrency-related investigation. For example, financial regulatory agencies use multiple complementary third-party tools to identify, trace, and attribute digital asset transactions on all major and most minor cryptocurrency and stablecoin blockchains. Currently, these tools support hundreds of tokens and use methods such as clustering algorithms, web scraping, and scam database monitoring that enable an investigator to link and attribute a wide range of transactions to real-world individuals and entities. The tools generate transaction graphs, which allow agencies to understand and then present the complex associations to juries and courts in subsequent prosecutions. Other regulators and law enforcement agencies use similar products from the private sector to help enhance the government's investigations and enforcement capabilities.

The Department also strongly supports information sharing between the private sector and the government, and will further explore the potential of such cooperation in the digital asset space. Existing initiatives designed to target the traditional financial sector could be expanded and adapted to ensure that they accommodate VASPs and other players in the digital asset sector. For instance, Section 314(a) of the Patriot Act requires the Secretary of the Treasury to adopt regulations to encourage regulatory and law enforcement

authorities to share with financial institutions information regarding individuals, entities, and organizations engaged in or reasonably suspected, based on credible evidence, of engaging in terrorist acts or money laundering activities. FinCEN established the 314(a) Program through the issuance of a rule (finalized in 2002 and, as amended, now at 31 C.F.R. Part 1010.520), which requires certain financial institutions to search their records and identify if they have responsive information with respect to the particular investigative subject. Under this program, an investigator can canvass the nation's financial institutions for potential lead information.

Complementing the 314(a) Program, Section 314(b) of the Patriot Act provides a safe harbor for financial institutions to share information with one another about activities that may involve money laundering or terrorist activites. In one successful collaboration, FBI investigators interfaced with a consortium of banks organized pursuant to Section 314(b) to analyze transactions related to a Hong Kong shell corporation that was being used as a front for a DPRK proliferation and sanctions evasion network, leading to the seizure and forfeiture of $1.9 million in illicit funds.[133] Similar efforts in the digital asset space could have significant impact.

The cooperative partnership between the financial community and law enforcement allows disparate bits of information to be identified, centralized, and rapidly evaluated. Expanded information sharing by financial institutions involved in digital assets-related products and services would be useful when investigating the use of such assets in criminal activity, especially as regulators and law enforcement continue to enforce regulations requiring digital asset exchanges to comply with KYC and AML/CFT rules.

FINCEN EXCHANGE AND IVAN

In recent years, FinCEN and the FBI have both instituted programs designed to enhance public-private partnerships in the digital assets space.

In December 2017, FinCEN launched the FinCEN Exchange, a voluntary public-private information sharing partnership among law enforcement, national security agencies, financial institutions, and FinCEN.[134] FinCEN Exchange was later formally established in Section 6103 of the Anti-Money-Laundering Act of 2020 (codified at 31 U.S.C. § 310(d)), which took effect in January 2021.

Through this program, FinCEN convenes briefings with law enforcement, FinCEN, and financial institutions to provide specific information on priority illicit finance and national security threats. To convene a briefing, FinCEN, in consultation with law enforcement, will invite financial institutions to voluntarily participate when FinCEN has reason to believe that the financial institution may have, or is capable of providing, information relevant to (or having an ability to support) a particular FinCEN Exchange briefing.[135] Such briefings can be subject-matter specific and have included participants from the digital assets industry.

One of the anticipated outcomes of FinCEN Exchange is that participating financial institutions take back the information received from briefings and, in a manner that the financial institution considers reasonable and proportionate pursuant to the financial institution's existing BSA procedures, report any suspicious activity relevant to the information shared. This enhanced reporting, in turn, assists in detecting, preventing, and prosecuting terrorism, organized crime, money laundering, and other financial crimes.[136]

Separately, the FBI, the National Cyber Investigative Joint Task Force, and FinCEN are working toward the establishment of the Illicit Virtual Asset Notification (IVAN) platform through which information about illicit activity involving digital assets can be shared with public and private IVAN partners. IVAN will provide a collaborative space between public and private partners to advance timely detection and disruption of the use of virtual assets in furtherance of illicit activity.[137]

IVAN is meant to serve as a two-way street to share actionable information. First, it will allow government agencies to share digital asset addresses affiliated with illicit activity with industry partners in as close to real-time as possible, and to identify for private industry participants a government point of contact to which they can direct responsive information. Second, it will provide a platform for industry participants to share information with the government or with other industry participants.

IV. LEGISLATIVE AND REGULATORY ACTIONS THAT COULD ENHANCE EFFORTS TO DISRUPT, INVESTIGATE, AND PROSECUTE CRIMINAL ACTIVITY RELATED TO DIGITAL ASSETS

Along with the *International Law Enforcement Cooperation Report*, Parts II and III above describe how U.S. law enforcement agencies have responded to the risks posed by the illicit use of digital assets and worked with international, regulatory, and private sector partners to successfully investigate and prosecute those who engage in criminal activity related to digital assets. The *International Law Enforcement Cooperation Report* likewise explained some of the significant obstacles encountered in digital assets-related investigations, including technological novelty that serves as a barrier to entry for some agents, analysts, prosecutors, and other attorneys; the need for early deconfliction of investigations at the domestic and international levels; and a cross-border evidence-gathering process that can be cumbersome and incomplete.

The Department recognizes, moreover, that law enforcement must expend substantial efforts to keep pace with rapidly changing technology in the digital assets space and ensure the type of domestic, international, and private-sector coordination necessary to disrupt criminal activity and confiscate ill-gotten gains for return to victims. Accordingly, and in response to the Executive Order's call for "any recommendations on regulatory or legislative actions," Part IV of this Report describes several legislative and regulatory actions that, in the Department's view, would facilitate efforts to investigate, prosecute, and otherwise disrupt digital asssets-related criminal activity.

These proposals are divided into five categories, beginning with the highest priority proposals and grouped by subject matter:

- The first category identifies three priority proposals that are integral to the continued success of prosecutions and other disruptions in the digital assets space: (1) extending the existing prohibition against disclosing subpoenas applicable to traditional financial institutions to VASPs that operate as money services businesses; (2) strengthening the federal law prohibiting operation of an unlicensed money transmitting business, which is a key prosecutorial tool in digital assets cases; and (3) extending the statute of limitations for crimes involving digital assets from five years to ten, as well as the period during which assistance requests to foreign governments toll the limitations period.

- The second category recommends support for other appropriate changes or initiatives that would aid investigators in gathering evidence and ensuring a suitable U.S. forum for prosecution.

- The third category proposes the facilitation of cryptocurrency forfeiture in appropriate cases and the strengthening of the Sentencing Guidelines applicable to certain BSA violations.

- The fourth category recommends advancing: (1) FinCEN's proposed amendments to the BSA's implementing regulations requiring covered financial institutions to collect and retain records about certain fund transfers or transmittals; and (2) any action that would ensure that the BSA's core AML/CFT requirements continue to apply appropriately to new technology as it develops, particularly with respect to platforms selling NFTs.

- The fifth category recommends ensuring that law enforcement and regulatory agencies receive the resources required to conduct—and staff—technologically sophisticated and data-driven digital assets-related investigations.

A. Priority Proposals

Investigations into digital assets-related crimes regularly involve a complex evidence-gathering process, a need to seek evidence from third parties domestically and abroad, and engagement with entities that play roles analogous to that of traditional financial institutions. Therefore, the Department supports the Administration prioritizing the following proposals: (1) expanding to VASPs the laws preventing employees of financial institutions from tipping off suspects to ongoing investigations; (2) strengthening the law criminalizing the operation of unlicensed money transmitting businesses; and (3) extending the statute of limitations period of certain statutes to account for the complexities of digital assets-related investigations.

1. Anti-Tip-Off Provision

Existing law makes it a crime for officers or agents of financial institutions to notify customers when their records are sought via grand jury subpoenas or certain other types of subpoenas seeking evidence of listed offenses.[138] These laws serve an important law enforcement function of deterring financial institutions from disclosing the existence of a criminal investigation to a customer who may have engaged in criminal activity—and who could thus take steps to destroy evidence or evade prosecution if tipped off about the investigation. Such deterrence is equally crucial for illicit activity in the digital assets space, where both individual customers and the entities that serve them may seek to leverage the privacy and perceived anonymity of transactions to further their criminal activity.

The definitions of "financial institution" that apply to the two statutes covering non-disclosure of subpoenas do not currently reach certain VASPs that operate as MSBs.[139] By contrast, there is a separate, broader definition of "financial institution" in the BSA that does cover these entities and imposes AML/CFT obligations upon them.[140] However, because these institutions are not included in the definition of "financial institution" in the statute governing subpoenas, no law prevents them from tipping off the subjects of criminal investigations when they receive a subpoena. This creates a significant gap in the non-disclosure framework for subpoenas in digital assets-related investigations. The Department supports legislation to eliminate this gap and ensure that VASPs operating as MSBs fall within the statutes' coverage.[141]

In addition, as currently written, the anti-tip-off prohibition in 18 U.S.C. § 1510(b) applies only to subpoenas related to an enumerated set of crimes—a list that omits serious offenses such as racketeering (18 U.S.C. § 1961), drug-trafficking offenses under Title 21, tax crimes under Title 26, securities violations under Title 15, computer crimes (18 U.S.C. § 1030), human trafficking, and

some mail and wire fraud schemes (18 U.S.C. §§ 1341, 1343). The Department supports consideration of proposals to further expand the covered offenses to include those listed here, or more generally to include all of Title 18, Title 21, and Chapter 53 of Title 31 (which contains the BSA), in light of the growing use of digital assets across a broad spectrum of criminal activities. Such an action would be consistent with Congress' recent expansion of the covered offenses to reach the operation of an unlicensed money transmitting business (18 U.S.C. § 1960).

2. Amendments to 18 U.S.C. § 1960 (Unlicensed Money Transmitting Businesses)

The Department may prosecute digital asset exchanges under 18 U.S.C. § 1960, which criminalizes the operation of an unlicensed money transmitting business. Any covered money transmitter that fails to register with FinCEN, fails to obtain the requisite state licensing, or otherwise transmits funds known to be criminally derived or destined to promote or support illicit activity may be subject to criminal prosecution under 18 U.S.C. § 1960. In light of the important role that § 1960 plays in digital assets investigations, the Department would welcome appropriate amendments that strengthen the law's penalty provisions and substantive reach.[142]

Investigations and prosecutions of suspected § 1960 violations involving digital assets have underscored several potential ways to strengthen the statute. The first pertains to § 1960's penalty provisions. Under existing law, violations of § 1960 are punishable by a maximum of five years' imprisonment, a term materially less than that prescribed for analogous fraud (20 or 30 years) and money laundering statutes (10 or 20 years).[143] Applicable Sentencing Guidelines ranges for § 1960, which are often calculated based on the volume of transactions, can easily exceed the five-year maximum and frequently do.[144] In addition, § 1960 violations are subject to the general fine provisions in Title 18, which provide for maximum fines of $250,000 for individuals, $500,000 for entities, or—in cases where the offender derives pecuniary gain from the offense—twice the amount of gross gain.[145] Other money laundering statutes, by contrast, provide for individual fines of $500,000 or twice the value of the funds involved in the transactions or transfer, whichever is greater (out of recognition that the amounts being laundered for others often dwarf the pecuniary gain to any individual launderer).[146] Enforcement efforts would benefit from increasing the statutory maximum sentence to 10 years (from five) and by adding an enhanced penalties provision, under which individual criminal fines would double—and corporate criminal fines would triple—for violations involving a money transmitter's business of more than $1 million in a 12-month period,[147] to reflect the seriousness of the conduct at issue and allow for sentences more in line with the Guidelines range called for by the Sentencing Commission.

Second, § 1960 and the regulations referenced in it must adequately address emerging technologies and new models for using digital assets. For example, the federal-registration prong (§ 1960(b)(1)(B)) turns on compliance "with the money transmitting business registration requirements under" the BSA or its implementing regulations.[148] Law enforcement investigations have revealed, however, that peer-to-peer platforms that profit by connecting buyers and sellers of cryptocurrencies have openly advertised the view that they fall outside of the BSA's AML/CFT regime, with some pointing to regulatory guidance that ties an entity's registration

obligations to, among other things, whether the entity takes custody or assumes control over the value to be exchanged.[149] The Department would welcome changes to clarify that the statute applies to platforms providing services that enable their users to transfer digital assets in a manner analogous to traditional money-transmitting businesses.

Third, and finally, there has been litigation in criminal cases regarding the requisite *mens rea* for a violation of the federal-registration prong (§ 1960(b)(1)(B)). The Department would welcome legislative actions that ratify existing case law holding that the same general intent requirement now found in the state-licensing prong (§ 1960(b)(1)(A)) also applies to the federal-registration prong (§ 1960(b)(1)(B)).[150]

3. Limitations Period for Crypto-Related Crimes

The default limitations period for non-capital federal offenses is five years under 18 U.S.C. § 3282. For certain enumerated offenses, and for mail- and wire-fraud offenses that affect "a financial institution," the statute of limitations is extended to 10 years, under 18 U.S.C. § 3293. The term "financial institution" in that provision carries the definition in 18 U.S.C. § 20, which does not include some key VASPs. Federal law separately provides for tolling or "suspension" of the limitations period, for a period of up to three years, while a foreign country responds to an official U.S. request for evidence in that country, under 18 U.S.C. § 3292.

In many cases, these provisions strike an adequate balance between, on the one hand, the time required to uncover and thoroughly investigate potential criminal conduct and, on the other, the interest of investigated persons in repose and certainty. Digital assets-related investigations, however, pose significant challenges analogous to those that have justified lengthier statutes of limitations periods in other contexts. These investigations can be complex and lengthy in duration, in part because their cross-border nature means that they require requests for mutual legal assistance from (often several different) foreign governments, which can take years to resolve. As a result, it is sometimes impracticable to identify the offender and bring charges within the standard five-year limitations period in 18 U.S.C. § 3282, even when that period is suspended pending a request for evidence abroad. Further, the longer 10-year period in 18 U.S.C. § 3293 is not necessarily available to prosecutors in digital assets-related cases, either because the conduct does not involve one of the enumerated offenses or because, as explained above, the entity affected by a fraudulent scheme does not qualify as a "financial institution" under current law.

To address these issues, the Department would welcome an amendment to 18 U.S.C. § 3293 to provide for a 10-year statute of limitations for all crimes (or an enumerated set of offenses) that involve the transfer of digital assets.[151] This amendment to § 3293 is recommended even if Congress were to expand the definition of "financial institution" to cover VASPs because such an expansion would affect only the class of mail- and wire-fraud crimes subject to a 10-year limitations period; it would not add offenses such as money laundering or BSA violations. In addition, the Department would welcome an amendment to 18 U.S.C. § 3292 to provide for a longer period of tolling (or "suspension") of the limitations period when the United States' official request to obtain foreign evidence pertains to an offense involving the transfer of digital assets.

B. Proposals to Facilitate Evidence Gathering and Ensure Appropriate Venue

Law enforcement's ability to timely collect evidence in cross-border digital assets cases is often hampered by disputes about records preservation and production. These include failures to preserve records; general delays in providing these records; attempts of some VASPs to withhold data requested by U.S. law enforcement agencies based on the European Union's General Data Privacy Regulation;[152] and, as described above, the length of time to obtain assistance through international requests for assistance. Issues also arise when cryptocurrency and hosting companies claim to be located everywhere and nowhere (personnel in one place, registration in another place, records in a third place) or in countries that are poorly positioned to respond quickly to requests for assistance (including mutual legal assistance treaty requests).

As a general matter, therefore, the Department recommends support for appropriate legislative and regulatory changes, as well as international-cooperation initiatives, designed to address the challenges in gathering evidence of crimes related to digital assets. Apart from the potential changes to the anti-tip-off provisions and limitations period described above, such changes and initiatives would include laws requiring record preservation or enhanced penalties for non-compliance with legal process.

Further, investigators require a forum for bringing digital assets-related charges that satisfies statutory and constitutional venue requirements without causing unnecessary hardship to victims. Identifying or bringing charges in such a forum, however, can be challenging in complex cybercrime cases, including those involving digital assets. Such cases will sometimes involve scenarios where the U.S.-based victim of the crime is far removed from the actors perpetrating the offense or from the location where the compromised financial account was hosted—locations that may themselves both be outside of the United States. In other words, a court may find that offense conduct did not occur in the district most likely to have investigated the crime, or in the United States at all.

To ensure a suitable venue for prosecution of digital assets-related crimes that harm the American public, the Department would welcome consideration of amendments to the venue provisions in Title 18—or to specific offenses in that or other titles of the U.S. Code—that would permit prosecution in any district where the victim of a digital assets-related offense or other cybercrime is found.

C. Proposals to Strengthen Penalties

Criminal laws best serve their deterrent purpose when punishment is both certain and sufficiently serious to discourage the targeted illicit activities. The Department's experience with digital assets-related cases, however, has revealed limits on the forfeiture tools used to deprive wrongdoers of ill-gotten gains and, in certain cases, restore funds to victims, as well as potential weaknesses in the penalties applicable to some provisions in the prosecutorial toolkit. Therefore, as described below, several updates to existing law should be sought to close gaps in the forfeiture laws and improve the Sentencing Guidelines governing some BSA violations.

1. Forfeiture Under 18 U.S.C. § 1348 and the Commodity Exchange Act

Cryptocurrencies and certain financial products related to them are considered commodities under federal law.[153] The Department can therefore charge fraud and manipulation in the cryptocurrency markets

under 18 U.S.C. § 1348 and 7 U.S.C. § 13(a)(2). But these statutes currently do not permit forfeiture of ill-gotten gains from criminal activity involving commodities.[154] Given the pervasiveness of fraud in the cryptocurrency markets, it is critical that the United States have the authority to forfeit the proceeds of cryptocurrency fraud and manipulation as a means of deterring such activity and divesting violators of their ill-gotten gains.

The Department would welcome amendments to provide criminal and civil forfeiture authority for commodities-related violations of 18 U.S.C. § 1348 (which covers both securities and commodities fraud) and 7 U.S.C. § 13(a)(2) (Commodity Exchange Act). That can be accomplished by listing commodities fraud under those two statutes in 18 U.S.C. § 1956(c)(7)(D), which defines the term "specified unlawful activity" for purposes of the money laundering statutes. Such an amendment would not only make these violations a predicate for money laundering charges, but would provide authorities for criminal and civil forfeiture of proceeds as well.

2. Lifting the Monetary Limit on Administrative Forfeiture of Cryptocurrency

Federal law has long provided that the Department can forfeit fruits of criminal activity not only by court order, but administratively.[155] The administrative forfeiture process promotes the efficient allocation of government resources, discourages undue burdens on the federal judicial system, and potentially expedites the return of funds to victims, while affording interested parties a prompt resolution through the remission process. Accordingly, Department policy recommends administrative forfeiture when available.[156]

Cryptocurrency investigations regularly involve assets with a high dollar value. Under 19 U.S.C. § 1607, with the exception of monetary instruments as defined in the BSA (31 U.S.C. § 5312(a)(3)), the availability of administrative forfeiture is capped at $500,000.[157] Section 6102(d) of the National Defense Authorization Act for Fiscal Year 2021[158] took a step toward addressing this by amending that definition of "monetary instruments" to include "value that substitutes for any monetary instrument"—but only insofar "as the Secretary [of the Treasury] shall provide by regulation." The Department recommends that Treasury exercise its authority to provide that cryptocurrency is a monetary instrument that is not subject to the $500,000 cap on administrative forfeiture. If Treasury does not do so, however, the Department would welcome an amendment to Section 1607 to lift the $500,000 cap for cryptocurrency and other digital assets.

3. Sentencing Guidelines for BSA Violations

The BSA is a critical part of the federal government's AML/CFT framework. Among other things, it imposes criminal penalties—including a sentence of imprisonment of up to five years—for covered entities that fail to implement an AML/CFT program or to submit SARs to Treasury.[159] The statutory maximum increases to ten years for willful violations committed while violating another federal law "or as part of a pattern of any illegal activity involving more than $100,000 in a 12-month period."[160]

For other money-laundering-related penalties in the U.S. Code (such as 18 U.S.C. §§ 1956, 1957, and 1960), the offense level under the advisory Sentencing Guidelines often rises as the amount of funds laundered or transferred increases.[161] That is not the case,

however, for BSA violations, despite the fact that the societal harm and systemic risks posed by non-compliant virtual currency exchanges and other MSBs rise with the scope and size of these entities' activities. The Guidelines provide for a base-offense level of 8 for BSA offenses, *see* U.S.S.G. § 2S1.3(a)(1), along with several possible enhancements based on specific offense characteristics and the generally applicable increases in Chapter 3 of the Guidelines (such as for the defendant's leadership role in the offense). Even with such enhancements, however, a defendant's Guidelines range for BSA-related violations always falls well below the five-year statutory maximum, even when the violations were widespread or facilitated millions of dollars' worth of money laundering. District courts, in turn, may end up viewing BSA offenses as mere technical or regulatory violations not meriting a substantial period of incarceration.

In light of these concerns, the Department is recommending to the Sentencing Commission that it consider amending U.S.S.G. § 2S1.3 to more accurately reflect the gravity of BSA violations that facilitate money laundering and other illicit activity. Changes could include the addition of specific offense characteristics tied to the nature of the BSA violations or, if a suitable metric for determining the value of the funds were identified, tying the base offense level to the amount of funds involved in or associated with the BSA violation.[162] Such amendments to the advisory Sentencing Guidelines would recognize that organizations with weak or non-existent BSA policies and programs in the digital assets industry facilitate the illicit use of digital assets and allow criminals to cash out or otherwise profit from their crimes.

D. Proposals Concerning the BSA and Its Implementing Regulations

As explained in Part III.B.1 above, the BSA and its implementing regulations are a crucial part of the framework for ensuring that criminals do not funnel funds through financial institutions for illicit purposes—and that institutions and regulators can identify wrongdoers who attempt to do so. To that end, the Department recommends: (1) providing appropriate support for a proposed FinCEN rule that would govern the transfer or transmission of certain digital assets; and (2) clarifying existing laws as necessary to ensure that NFT platforms are subject to the AML/CFT and suspicious-activity-reporting requirements of the BSA.

1. Recordkeeping and Travel Rule Under the BSA

The BSA and its implementing regulations require covered financial institutions to collect and retain records about certain fund transfers or transmittals and to pass on particular information to other financial institutions involved in the transfer or transmittal. This latter requirement is known as the "travel rule." In October 2020, FinCEN—partly in conjunction with the Board of Governors of the Federal Reserve—initiated a proposed rulemaking to amend the recordkeeping and travel rule regulations under the BSA.[163] Among other things, the proposed amendment clarifies that the recordkeeping and travel rule regulations apply to transactions above the applicable threshold involving convertible virtual currency, as well as transactions involving digital assets with legal tender status.

The Department supports FinCEN's issuance of a final rule, which is a necessary step to meeting the objectives that the rule is designed to achieve—including mitigating the illicit finance risks posed by digital assets by preserving information about their transaction.[164] Once FinCEN issues the final rule, the Department proposes to support FinCEN in enforcing the rule and encouraging its implementation throughout the digital assets industry.

2. Application of the BSA to NFT Platforms

Recent years have seen explosive growth in the demand and corresponding markets for NFTs, perhaps most notably in the area of digital art. The increased trade in NFTs, however, presents substantial money-laundering risks. As explained in a recent Treasury study, NFTs can be used to conduct self-laundering, a sequence in which criminals purchase an NFT with illicit funds and then resell to a purchaser who pays for it with clean funds unconnected to a prior crime.[165] In addition, the characteristics of digital art and the nature of the market—including the ability to trade purchased works repeatedly during a short period for immediate profit—have created an environment in which NFT platforms do not always carry out effective customer identification.[166] Under the current statutory and regulatory regime, the BSA's application often turns on whether the transacted item qualifies as "value that substitutes for currency."[167] NFT platforms may take the view that this definition does not apply to their activities—and that they are thus not subject to the BSA's AML/CFT requirements.

To address these potential gaps, the Department supports amendments to the BSA and its implementing regulations to the extent needed to make clear that its key AML/CFT provisions— including the obligations to have customer identification programs and report suspicious transactions to regulators—apply to NFT platforms, including online auction houses and digital art galleries.

E. Proposal to Ensure Adequate Funding of Law Enforcement Operations

Investigations into the illicit use of digital assets are often technologically sophisticated, resource-intensive, and may benefit from tools developed by private blockchain analysis companies, such as those described in Part III.C above. To ensure that the law enforcement and regulatory agencies keep pace with changing technologies, the Department recommends that adequate funding be pursued through the budgetary process and that hiring authorities be maximized to ensure the caliber of investigative personnel required for this class of investigations.

Like other federal agencies, the Department faces several resource-related challenges in developing and maintaining its expertise in detecting, investigating, and prosecuting digital assets related crimes. To start, sophisticated digital asset investigations are often data-driven, requiring (1) computing systems capable of storing and sorting massive amounts of information; and (2) access to blockchain analytical tools, many of which are proprietary technologies provided by private companies. But technology of this nature is costly, with licenses for proprietary blockchain analytical tools being particularly expensive. Many Department components are therefore able to provide investigators and prosecutors with only a limited number of such licenses, thereby creating a bottleneck of investigative resources.

In addition, the Department has faced challenges in training and retaining investigators and prosecutors to handle complex cryptocurrency matters. The technology associated with digital assets cases remains novel for some agents, analysts, and prosecutors, requiring a significant investment of time and resources to develop expertise in the field. Because that expertise is in high demand in the private sector, agents, analysts, prosecutors, and other attorneys who develop that expertise are regularly offered more lucrative employment opportunities outside of government. Multiple Department components—and the Department's regulatory and law enforcement partners—have therefore reported substantial challenges in retaining qualified personnel.

The Department recommends addressing these challenges through at least two avenues. First, the President's budget should seek funding from Congress for additional tools and technical resources specific to digital assets that can support investigations and search-and-seizure operations, including blockchain analytical tools and the technical infrastructure (*e.g.*, server space or cloud access) needed to ingest and maintain potentially voluminous and complex data and to analyze that data. Second, the Department and other government agencies should redouble their efforts to hire and retain the skilled agents, analysts, prosecutors, and other attorneys essential to addressing existing and emerging threats relating to digital assets. As explained in the recent *Comprehensive Cyber Review* report,[168] authorities already conferred by Congress can be used to draw technology-oriented personnel into federal service and keep them there, including through bonus compensation, increased leave accrual, and hiring directly into roles in the Senior Executive Service. But should these existing mechanisms prove insufficient given private sector competition in the digital asset space, the Department and other government agencies would benefit from additional authorities from Congress as appropriate.

CONCLUSION

The emerging technologies and markets associated with the rise of digital assets have created new opportunities for criminal actors to harm individual victims, avoid regulation, evade economic sanctions, raise funds for terrorist activities, and launder ill-gotten gains. The Department and its law enforcement and regulatory partners have long been at the forefront of efforts to detect, investigate, prosecute, and otherwise disrupt digital assets-related crimes, and to divest wrongdoers of their illegal gains. Although the Department is dedicated to and adept at addressing technologically advanced criminal activity, substantial budgetary, legislative, and regulatory efforts will be required to keep pace with, and protect victims from the abuse of, rapidly changing technology in the digital assets space. Regardless, as the markets for and uses of digital assets evolve, the Department and its partners will respond by efficiently deploying the expertise gained in recent years and utilizing existing resources to train new generations of agents, analysts, prosecutors, and other attorneys capable of using all tools at their disposal to mitigate risks in this space and bring wrongdoers to justice.

ENDNOTES

[1] U.S. Dep't of Justice, Report of the Attorney General's Cyber-Digital Task Force (2018) [hereinafer *2018 Cyber-Digital Task Force Report*], https://www.justice.gov/archives/ag/page/file/1076696/download.

[2] U.S. Dep't of Justice, Report of the Attorney General's Cyber-Digital Task Force: *Cryptocurrency Enforcement Framework* (2020) [hereinafter *Cryptocurrency Enforcement Framework*], https://www.justice.gov/archives/ag/page/file/1326061/download.

[3] U.S. Dep't of Justice, The Report of the Attorney General Pursuant to Section 8(b)(iv) of Executive Order 14067: How To Strengthen International Law Enforcement Cooperation For Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets (2022) [hereinafter *International Law Enforcement Cooperation Report*], https://www.justice.gov/ag/page/file/1510931/download.

[4] *2018 Cyber-Digital Task Force Report*, *supra* note 1, at 54; *Cryptocurrency Enforcement Framework*, *supra* note 2, at 2-3; *see also* Majority Staff of U.S. S. Comm. on Homeland Sec. & Governmental Affs., 117th Cong., Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns 15 (2022) (noting that "there is no uniform definition of 'cryptocurrency' under U.S. law," and that "'[c]ryptocurrency' is often referred to as 'virtual currency,' 'digital assets,' 'digital tokens,' 'cryptoassets,' or 'crypto'"), https://www.hsgac.senate.gov/imo/media/doc/HSGAC%20Majority%20Cryptocurrency%20Ransomware%20Report_Executive%20Summary.pdf; Joint Statement, Heath Tarbert, Kenneth A. Blanco, Jay Clayton, *Leaders of CFTC, FinCEN, and SEC Issue Joint Statement on Activities Involving Digital Assets* at n.4 (Oct. 11, 2019) (recognizing that "market participants refer to digital assets using many different labels"), https://www.fincen.gov/sites/default/files/2019-10/CVC%20Joint%20Policy%20Statement_508%20FINAL_0.pdf.

[5] *See, e.g.*, U.S. Dep't of Treasury, Fin. Crimes Enf't Network, FIN-2019-G001, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

[6] Financial Action Task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* at 21, 109 (Oct. 2021) (defining "virtual asset" as a "digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes"), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf; *see also id*. at 22, 109 (defining "virtual asset service provider" as any natural or legal person that as a business conducts one of the following activities or operations for or on behalf of another natural or legal person: (i) exchange between virtual assets and fiat currencies; (ii) exchange between one or more forms of virtual assets; (iii) transfer of virtual assets; (iv) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and (v) participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset).

[7] *See* Exec. Order No. 14067, 87 Fed. Reg. 14143, 14151-152 (Sec. 9(d)) (Mar. 14, 2022) ("The term 'digital assets' refers to all [Central Bank Digital Currencies (CBDCs)], regardless of the technology used, and to other representations of value, financial assets and instruments, or claims that are used to make payments or investments, or to transmit or exchange funds or the equivalent thereof, that are issued or represented in digital form through the use of distributed ledger technology. For example, digital assets include cryptocurrencies, stablecoins, and CBDCs. Regardless of the label used, a digital asset may be, among other things, a security, a commodity, a derivative, or other financial product. Digital assets may be exchanged across digital asset trading platforms, including centralized and so-called decentralized finance platforms, or through peer-to-peer technologies.").

[8] *Id*. at 14151 (Sec. 9(c)). The Executive Order defines the term "blockchain," in turn, as "distributed ledger technologies where data is shared across a network that creates a digital ledger of verified transactions or information among network participants and the data are typically linked using cryptography to maintain the integrity of the ledger and execute other functions, including transfer of ownership or value." *Id*., at 14152 (Sec. 9(a)).

[9] *See International Law Enforcement Cooperation Report*, *supra* note 3, at 26-27; Press Release, *Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges*, U.S. Dep't of Justice (July 21, 2008), https://www.justice.gov/archive/opa/pr/2008/July/08-crm-635.html; Press Release, *Liberty Reserve Founder Sentenced to 20 Years For Laundering Hundreds of Millions of Dollars*, U.S. Dep't of Justice (May 6, 2016), https://www.justice.gov/opa/pr/liberty-reserve-founder-sentenced-20-years-laundering-hundreds-millions-dollars.

[10] This Report follows the convention of referring to "the Bitcoin network and its protocols . . . with a capital B, while the units transmitted on the network are referred to with a lowercase b." *United States v. Harmon*, 474 F. Supp. 3d 76, 81 (D.D.C. 2020).

[11] Press Release, *Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace*, U.S. Dep't of Justice (Apr. 5, 2022), https://www.justice.gov/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace. When this Report references or describes criminal cases that are pending (such as this one), it should be noted that criminal charges are merely allegations and that all defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law. Additionally, unless otherwise noted, descriptions of cryptocurrency values refer to their valuations at the time of the asset seizure or other law enforcement action.

[12] Press Release, *Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex*, U.S. Dep't of Treasury (Apr. 5, 2022), https://home.treasury.gov/news/press-releases/jy0701.

[13] Federal Bureau of Investigation, *Internet Crime Report 2021* at 14, https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

[14] *See* Chainalysis, *The 2022 Crypto Crime Report* at 38 (Feb. 2022) (estimating more than $692 million ransomware payments made in 2020).

[15] FBI, *Internet Crime Report 2021*, *supra* note 13, at 15-16; *see, e.g*., Press Release, *Justice Department Seizes and Forfeits Approximately $500,000 from North Korean Ransomware Actors and their Conspirators*, U.S. Dep't of Justice (July 19, 2022), https://www.justice.gov/opa/pr/justice-department-seizes-and-forfeits-approximately-500000-north-korean-ransomware-actors.

[16] Press Release, *Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside,* U.S. Dep't of Justice (June 7, 2021), https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

[17] *See* U.S. Dep't of Treasury, *National Strategy for Combating Terrorist and Other Illicit Financing* 27 (2022) (stating that "some terrorist groups and their supporters have used, or are seeking to use, virtual assets"), https://home.treasury.gov/system/files/136/2022-National-Strategy-for-Combating-Terrorist-and-Other-Illicit-Financing.pdf.

[18] *See Cryptocurrency Enforcement Framework, supra* note 2, at 11-12.

[19] Press Release, *Grand Jury Indicts 12 Russion Intelligence Officers for Hacking Offenses Related to the 2016 Election*, U.S. Dep't of Justice (July 13, 2018), https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election.

[20] *See, e.g.*, Press Release, *Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency From Exchange Hack*, U.S. Dep't of Justice (Mar. 2, 2020), https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack; Press Release, *United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied to Hacks of Two Exchanges by North Korean Actors*, U.S. Dep't of Justice (Aug. 27, 2020), https://www.justice.gov/opa/pr/united-states-files-complaint-forfeit-280-cryptocurrency-accounts-tied-hacks-two-exchanges; Press Release, *Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe*, U.S. Dep't of Justice (Feb. 17, 2021), https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

[21] *See International Law Enforcement Cooperation Report*, *supra* note 3, at 23; Steven Zeitchik, *Hackers hit popular video game, stealing more than $600 million in cryptocurrency*, Wash. Post (March 29, 2022), https://www.washingtonpost.com/technology/2022/03/29/axie-infinity-cryptocurrency-hack/.

[22] The term "smart contracts," as used in the Report, refers to code that is deployed on a blockchain and that, if activated by a transaction on the blockchain, "will be executed through the blockchain's network of computers and will produce a change in the blockchain's 'state.'" Int'l. Org. of Sec. Comm'ns, Decentralized Finance Report 5 (2022) [hereinafter *IOSCO DeFi Report*], https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf.

[23] *Cryptocurrency Enforcement Framework*, *supra* note 2, at 41; *see, e.g.*, Complaint, *United States v. Nguyen and Llacuna*, No. 22 Mag. 2478, at 16-17 (S.D.N.Y. Mar. 15, 2022), https://www.justice.gov/usao-sdny/press-release/file/1486816/download.

[24] U.S. Dep't of Treasury, *2022 National Money Laundering Risk Assessment* at 40-41 (Feb. 2022), https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf.

[25] *See International Law Enforcement Cooperation Report*, *supra* note 3, at 1-2, 11. However, even VASPs ostensibly located outside the United States may still have obligations under the BSA if they qualify as domestic financial institutions, including by doing business wholly or in substantial part in the United States. *See, e.g.*, 31 C.F.R. § 1010.100(f).

[26] U.S. Dep't of Treasury, Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art 25-27 (2022), https://home.treasury.gov/system/files/136/Treasury_Study_WoA.pdf; *see also* Elliptic, Typologies Report: Preventing Financial Crime in *Cryptoassets* at 82 (2022 ed.), https://www.elliptic.co/hubfs/Typologies-2022-Preventing%20Financial%20Crime%20in%20Crypto-NH.pdf?hsCtaTracking=459bfdd0-05d4-4c16-ade1-d73d88236fe8%7Ce1df3ed3-2a59-40bc-990d-a11d6a803e24.

[27] Press Release, *Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency*, U.S. Dep't of Justice (Feb. 8, 2022), https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.

[28] Press Release, *Ohio Resident Pleads Guilty to Operating Darknet-Based Bitcoin 'Mixer' That Laundered Over $300 Million*, U.S. Dep't of Justice (Aug. 18, 2021), https://www.justice.gov/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million.

[29] Press Release, *Ohio Resident Charged with Operating Darknet-Based Bitcoin 'Mixer,' which Laundered Over $300 Million*, U.S. Dep't of Justice (Feb. 13, 2020), https://www.justice.gov/opa/pr/ohio-resident-charged-operating-darknet-based-bitcoin-mixer-which-laundered-over-300-million.

[30] Press Release, *First Bitcoin "Mixer" Penalized by FinCEN for Violating Anti-Money Laundering Laws*, U.S. Dep't of Treasury, Fin. Crimes Enf't Network (Oct. 19, 2020), https://www.fincen.gov/news/news-releases/first-bitcoin-mixer-penalized-fincen-violating-anti-money-laundering-laws.

[31] Chainalysis, *The 2022 Crypto Crime Report*, *supra* note 14, at 70.

[32] *Id*. at 70-72.

[33] *Id*. at 79.

[34] Emma Fletcher, *Reports of Romance Scams Hit Record Highs in 2021*, Fed. Trade Comm'n (Feb. 10, 2022), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/02/reports-romance-scams-hit-record-highs-2021#_ednref1.

[35] *See Consumer Complaint Database*, Consumer Fin. Prot. Bureau, https://www.consumerfinance.gov/data-research/consumer-complaints/search/?chartType=line&dateInterval=Month&date_received_max=2021-12-31&date_received_min=2021-01-01&lens=Overview&product=Money%20transfer%2C%20virtual%20currency%2C%20or%20money%20service%E2%80%A2Virtual%20currency&searchField=all&tab=Trends (2021 data); https://www.consumerfinance.gov/data-research/consumer-complaints/search/?chartType=line&dateInterval=Month&date_received_max=2022-07-29&date_received_min=2022-01-01&lens=Overview&product=Money%20transfer%2C%20virtual%20currency%2C%20or%20money%20service%E2%80%A2Virtual%20currency&searchField=all&tab=Trends (2022 year-to-date data). The CFPB publishes complaints sent to companies for response in the Consumer Complaint Database after the company responds, confirming a commercial relationship with the consumer, or after 15 days, whichever comes first. Other complaints that cannot be sent to companies for response, such as complaints about scammers, are not eligible for publication.

[36] *IOSCO DeFi Report*, *supra* note 22, at 21.

[37] *International Law Enforcement Cooperation Report*, *supra* note 3, at 22; *2022 National Money Laundering Risk Assessment*, *supra* note 24, at 42; *What is DeFi?*, coinbase, https://www.coinbase.com/learn/crypto-basics/what-is-defi. One of the more unusual DeFi projects was the ConstitutionDAO, a single-purpose decentralized autonomous organization (DAO) formed for the purpose of acquiring one of the original copies of the U.S. Constitution, a process that would have involved raising money to bid on the item at auction and, if successful, obtaining insurance and finding facilities to house the historical artifact. *See* Andrew Thurman, *'I Think We're Doing This': Inside One DAO's $20M Plot to Purchase the US Constitution*, CoinDesk (Nov. 15, 2021), https://www.coindesk.com/tech/2021/11/15/i-think-were-doing-this-inside-one-daos-20m-plot-to-purchase-the-us-constitution/. Ultimately, however, the DAO was outbid at an auction and soon announced plans to disband. *See* Jacob Kastrenakes, *ConstitutionDAO will shut down after losing bid for Constitution*, The Verge (Nov. 23, 2021), https://www.theverge.com/2021/11/23/22799192/constitutiondao-shutting-down-lost-auction-refunds.

[38] For instance, DeFi platforms may be subject to BSA obligations, including if they qualify as MSBs or otherwise fall under the BSA definition of a financial institution (a term that reaches, among other things, futures commission merchants subject to CFTC supervision).

[39] *See* Gary Silverman, *Cryptocurrency: rise of decentralized finance sparks 'dirty money' fears*, FIN. TIMES (Sept. 15, 2021), https://www.ft.com/content/beeb2f8c-99ec-494b-aa76-a7be0bf9dae6; William Foxley, *ShapeShift Is Going Full DeFi to Lose KYC Rules*, COINDESK (Jan. 6, 2021), https://www.coindesk.com/business/2021/01/06/shapeshift-is-going-full-defi-to-lose-kyc-rules/.

[40] *See, e.g.*, Sam Reynolds, *Tornado Cash Co-Founder Says the Mixer Protocol Is Unstoppable*, COINDESK (Jan. 25, 2022), https://www.coindesk.com/tech/2022/01/25/tornado-cash-co-founder-says-the-mixer-protocol-is-unstoppable/; Sam Bourgi, *Controversial mixer Tornado Cash open-sources UI code*, COINTELEGRAPH (July 7, 2022), https://cointelegraph.com/news/controversial-mixer-tornado-cash-open-sources-ui-code.

[41] Chainalysis, *The 2022 Crypto Crime Report*, *supra* note 14, at 30; *see also NFT*, COINBASE, https://help.coinbase.com/en/coinbase/getting-started/crypto-education/glossary/nft. NFTs can be tokenized, traded like securities or commodities, and in some instances may function as substitutes of value.

[42] U.S. GOV'T ACCOUNTABILITY OFF., GAO-22-105990, SCIENCE & TECH SPOTLIGHT: NON-FUNGIBLE TOKENS (NFTS) (2022), https://www.gao.gov/products/gao-22-105990.

[43] Chainalysis, *The 2022 Crypto Crime Report*, *supra* note 14, at 30.

[44] *See, e.g.*, Joel Khalili, *Hundreds of NFTs stolen from OpenSea wallets – here's what you need to know*, TECHRADAR (Apr. 14, 2022), https://www.techradar.com/news/hundreds-of-nfts-stolen-from-opensea-wallets-heres-what-you-need-to-know; David Yaffe-Bellany, *Thefts, Fraud and Lawsuits at the World's Biggest NFT Marketplace*, N.Y. TIMES (June 6, 2022), https://www.nytimes.com/2022/06/06/technology/nft-opensea-theft-fraud.html; Edward Ongweso Jr., *'All My Apes Gone': NFT Theft Victims Beg for Centralized Saviors*, VICE (Jan. 6, 2022), https://www.vice.com/en/article/y3v3ny/all-my-apes-gone-nft-theft-victims-beg-for-centralized-saviors.

[45] *See, e.g.*, Chainalysis, *The 2022 Crypto Crime Report*, *supra* note 14, at 31-35; ELLIPTIC, TYPOLOGIES REPORT: PREVENTING FINANCIAL CRIME IN CRYPTOASSETS 82 (2022 ed.), *supra* note 26, at 82-87; Marco Quiroz-Gutierrez, *Not even crypto's biggest names are safe as NFT marketplace OpenSea's Discord channels infiltrated by a hacker promoting a scam drop*, FORTUNE (May 6, 2022), https://fortune.com/2022/05/06/opensea-discord-hacked-nfts-stolen-phishing-scams/.

[46] *See* Chainalysis, *The 2022 Crypto Crime Report*, *supra* note 14, at 35-36.

[47] Press Release, *Former Employee of NFT Marketplace Charged in First Ever Digital Asset Insider Trading Scheme*, U.S. Dep't of Justice (June 1, 2022), https://www.justice.gov/usao-sdny/pr/former-employee-nft-marketplace-charged-first-ever-digital-asset-insider-trading-scheme.

[48] Press Release, *Three Charged In First Ever Cryptocurrency Insider Trading Tipping Scheme*, U.S. Dep't of Justice (July 21, 2022), https://www.justice.gov/usao-sdny/pr/three-charged-first-ever-cryptocurrency-insider-trading-tipping-scheme. On the same day, the SEC filed a parallel complaint alleging insider trading. *See* Press Release, *SEC Charges Former Coinbase Manager, Two Others in Crypto Asset Insider Trading Action*, SEC (July 21, 2022), https://www.sec.gov/news/press-release/2022-127.

[49] Press Release, *Digital Currency Business E-Gold Indicted For Money Laundering And Illegal Money Transmitting*, U.S. Dep't of Justice (Apr. 27, 2007), https://www.justice.gov/archive/criminal/cybercrime/press-releases/2007/egoldIndict.htm; Press Release, *In U.S. Secret Service-Led Investigation, Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges*, U.S. Secret Service (July 22, 2008), https://www.secretservice.gov/press/releases/2008/07/us-secret-service-led-investigation-digital-currency-business-e-gold-pleads.

[50] Press Release, *Liberty Reserve Founder Sentenced to 20 Years For Laundering Hundreds of Millions of Dollars*, U.S. Dep't of Justice (May 6, 2016), https://www.justice.gov/opa/pr/liberty-reserve-founder-sentenced-20-years-laundering-hundreds-millions-dollars; *see* Press Release, *Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One Of World's Largest Digital Currency Companies, And Seven Of Its Principals And Employees For Allegedly Running A $6 Billion Money Laundering Scheme*, U.S. Dep't of Justice (May 28, 2013), https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-liberty-reserve-one-world-s-largest.

[51] *See International Law Enforcement Cooperation Report*, *supra* note 3, at 28 & n.46; *United States v. Ulbricht*, 858 F.3d 71, 82-83 & n.1 (2d Cir. 2017).

[52] *2020 Cryptocurrency Enforcement Framework*, *supra* note 2, at 49.

[53] *2018 Cyber-Digital Task Force Report*, *supra* note 1, at 41, 53-56, 126.

[54] *2020 Cryptocurrency Enforcement Framework*, *supra* note 2, at 20-52.

[55] U.S. Dep't of Justice, Comprehensive Cyber Review 29-30 (2022), https://www.justice.gov/dag/page/file/1520341/download.

[56] Press Release, *Deputy Attorney General Lisa O. Monaco Delivers Remarks at Annual Munich Cyber Security Conference*, U.S. Dep't of Justice (Feb. 17, 2022), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-annual-munich-cyber-security.

[57] *See International Law Enforcement Cooperation Report*, *supra* note 3, at 39.

[58] *2018 Cyber-Digital Task Force Report*, *supra* note 1, at 100.

[59] *Id*. at 102.

[60] Press Release, *Justice Department Seizes and Forfeits Approximately $500,000 from North Korean Ransomware Actors and their Conspirators*, U.S. Dep't of Justice (July 19, 2022), https://www.justice.gov/opa/pr/justice-department-seizes-and-forfeits-approximately-500000-north-korean-ransomware-actors.

[61] Press Release, *Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside*, U.S. Dep't of Justice (June 7, 2021), https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

[62] Press Release, *Justice Department Announces Enforcement Action Charging Six Individuals with Cryptocurrency Fraud Offenses in Cases Involving Over $100 Million in Intended Losses*, U.S. Dep't of Justice (June 30, 2022), https://www.justice.gov/opa/pr/justice-department-announces-enforcement-action-charging-six-individuals-cryptocurrency-fraud.

[63] In addition, the CFTC and SEC both filed actions related to the scheme. Press Release, *CFTC Charges Commodity Pool Operators and a Florida Company with Fraudulently Solicitating Over $41.6 Million in a Commodity Pool Scheme*, CFTC (June 30, 2022), https://www.cftc.gov/PressRoom/PressReleases/8551-22; Press Release, *SEC Charges Empires Consulting Corp. with Fake Trading Scheme*, SEC (June 30, 2022), https://www.sec.gov/news/press-release/2022-119.

[64] In addition, the CFTC filed an action related to the scheme. Press Release, *Federal Court Orders Nevada Company and its Owner to Pay More Than $32 Million for Cryptocurrency Fraud and Misappropriation Scheme*, CFTC (April 8, 2021), https://www.cftc.gov/PressRoom/PressReleases/8377-21.

[65] The SEC filed a parallel civil action. Press Release, *SEC Obtains Emergency Order Halting Fraudulent Coin Offering Scheme*, SEC (May 29, 2018), https://www.sec.gov/news/press-release/2018-94.

[66] HSI's AFU has initiated a Virtual Assets Recovery Program to streamline the seizure and forfeiture of cryptocurrency by obtaining and utilizing HSI controlled digital wallets to assist field offices in securing digital assets for safe transfer to AFU. AFU then monitors the asset through the forfeiture process, including the ultimate transfer to the Marshals Service for liquidation.

[67] Press Release, *U.S. Secret Service Launches Cryptocurrency Awareness Hub*, U.S. Secret Service (Feb. 18, 2022), https://www.secretservice.gov/newsroom/releases/2022/02/us-secret-service-launches-cryptocurrency-awareness-hub.

[68] U.S. Secret Service, *Combating the Illicit Use of Digital Assets*, https://www.secretservice.gov/investigation/DigitalAssets.

[69] Press Release, *Founders of Crypto ICO Sentenced to Combined 8 Years in Prison for Tax Evasion After Raising $24 Million from Investors*, U.S. Dep't of Justice (March 10, 2022), https://www.justice.gov/usao-ndtx/pr/founders-crypto-ico-sentenced-combined-8-years-prison-tax-evasion-after-raising-24.

[70] Press Release, *SEC Charges Dallas Company and Its Founders with Defrauding Over 13,000 Investors in Unregistered Offering and Operating Unregistered Digital Asset Exchange*, SEC (Aug. 29, 2019), https://www.sec.gov/news/press-release/2019-164.

[71] IRS:CI, Annual Report 2021 8 (2021), https://www.irs.gov/pub/irs-pdf/p3583.pdf.

[72] *2020 Cryptocurrency Enforcement Framework*, *supra* note 2, at 23.

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

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

[75] U.S. Dep't of Treasury, Fin. Crimes Enf't Network, FIN-2019-G001, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, *supra* note 5. FinCEN's guidance notes that while the "term 'virtual currency' refers to a medium of exchange that can operate like currency," virtual currency "does not have all the attributes of 'real' currency, as defined by 31 CFR § 1010.100(m), including legal tender status." *Id.* (citing U.S. Dep't of Treasury, Fin. Crimes Enf't Network, FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (2013)). *See also 2020 Cryptocurrency Enforcement Framework*, *supra* note 2, at 2-3.

[76] *See* Press Release, *Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange*, U.S. Dep't of Treasury (Nov. 8, 2021), https://home.treasury.gov/news/press-releases/jy0471. A "nested" exchange is one that does "not have direct custody of its clients' cryptocurrency but instead use[s] the infrastructure of a larger multinational exchange." Derrick Kyle & Olga Torres, *Crypto Crackdown: OFAC Sanctions SUEX Cryptocurrency Exchange*, JD Supra (Oct. 27, 2021), https://www.jdsupra.com/legalnews/crypto-crackdown-ofac-sanctions-suex-3337719/.

[77] Press Release, *Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex*, U.S. Dep't of Treasury (Apr. 5, 2022), https://home.treasury.gov/news/press-releases/jy0701.

[78] Press Release, *U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats*, U.S. Dep't of Treasury (May 6, 2022), https://home.treasury.gov/news/press-releases/jy0768.

[79] Press Release, *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*, U.S. Dep't of Treasury (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916.

[80] U.S. Dep't of Treasury, *Sanctions Compliance Guidance for the Virtual Currency Industry* (Oct. 2021), https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf (last viewed April 25, 2022).

[81] *See e.g.*, U.S. Dep't of Treasury, *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Oct. 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf; U.S. Dep't of the Treasury, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Sept. 21, 2021), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.

[82] *In re Criminal Complaint*, No. 22-mj-067, 2022 WL 1573361 (D.D.C. May 13, 2022).

[83] U.S. Dep't of Treasury, *Sanctions Compliance Guidance for the Virtual Currency Industry*, *supra* note 80, at 1 (emphasis added).

[84] *In re Criminal Complaint*, 2022 WL 1573361, at *4.

[85] Enforcement Release, Dep't of Treasury, *OFAC Enters Into $98,830 Settlement with BitGo, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions* (Dec. 30, 2020), https://home.treasury.gov/system/files/126/20201230_bitgo.pdf.

[86] Enforcement Release, Dep't of Treasury, *OFAC Enters Into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions* (Feb. 18, 2021), https://home.treasury.gov/system/files/126/20210218_bp.pdf.

[87] Press Release, *United States Citizen Who Conspired To Assist North Korea In Evading Sanctions Is Sentenced To More Than 5 Years And Fined $100,000*, U.S. Dep't of Justice (Apr. 12, 2022), https://www.justice.gov/usao-sdny/pr/united-states-citizen-who-conspired-assist-north-korea-evading-sanctions-sentenced-more.

[88] *2020 Cryptocurrency Enforcement Framework*, *supra* note 2, at 29-30.

[89] U.S. Sec. and Exch. Comm'n, *Release No. 81207: Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* 10 (July 25, 2017), at: https://www.sec.gov/litigation/investreport/34-81207.pdf.

[90] *Id.*; *see also* U.S. Sec. & Exch. Comm'n Staff, *Framework for Investment Contract Analysis of Digital Assets*, https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.

[91] The term "security" is defined in Section 2(a)(1) of the Securities Act of 1933, Section 3(a)(10) of the Securities Exchange Act of 1934, Section 2(a)(36) of the Investment Company Act of 1940, and Section 202(a)(18) of the Investment Advisers Act of 1940.

[92] *SEC v. W. J. Howey Co.*, 328 U.S. 293, 301 (1946).

[93] *SEC v. Kik Interactive Inc.*, No. 19-cv-5244 (S.D.N.Y. Sept. 30, 2020).

[94] *Id.* at 18.

[95] SEC, Strategic Hub for Innovation and Financial Technology (FinHub), www.sec.gov/finhub.

[96] Press Release, *BlockFi Agrees to Pay $100 Million in Penalties and Pursue Registration of its Crypto Lending Product*, SEC (Feb. 14, 2022), https://www.sec.gov/news/press-release/2022-26.

[97] Press Release, *SEC Charges Decentralized Finance Lender and Top Executives for Raising $30 Million Through Fraudulent Offerings*, SEC (Aug. 6, 2021), https://www.sec.gov/news/press-release/2021-145.

[98] Press Release, *Founder of Fraudulent Cryptocurrency Charged in $2 Billion BitConnect Ponzi Scheme*, Dept. of Justice, U.S. Att'y's Off., S.D. Cal. (Feb. 25, 2022), https://www.justice.gov/usao-sdca/pr/founder-fraudulent-cryptocurrency-charged-2-billion-bitconnect-ponzi-scheme.

[99] Press Release, *Director and Promoter of BitConnect Pleads Guilty in Global $2 Billion Cryptocurrency Scheme*, U.S. Dep't of Justice (Sept. 1, 2021), https://www.justice.gov/usao-sdca/pr/director-and-promoter-bitconnect-pleads-guilty-global-2-billion-cryptocurrency-scheme.

[100] Press Release, *SEC Charges Global Crypto Lending Platform and Top Executives in $2 Billion Fraud*, SEC (Sept. 1, 2021), https://www.sec.gov/news/press-release/2021-172.

[101] Press Release, *SEC Nearly Doubles Size of Enforcement's Crypto Assets and Cyber Unit*, SEC (May 3, 2022), https://www.sec.gov/news/press-release/2022-78 .

[102] 7 U.S.C. §§ 2(a)(1)(A), 9(1); *see also 2020 Cryptocurrency Enforcement Framework*, *supra* note 2, at 32-33.

[103] 7 U.S.C. § 1a(9).

[104] The CFTC defines the term virtual or digital asset as one that encompasses any digital representation of value that functions as a medium of exchange, and any other digital unit of account that is used as a form of a currency (*i.e.*, transferred from one party to another as a medium of exchange); may be manifested through units, tokens, or coins, among other things; and may be distributed by way of digital 'smart contracts,' among other structures. The Commission, however, has not created a bright line definition given the evolving nature of the commodity.

[105] *In re Coinflip, Inc.*, CFTC No. 15-29, 2015 WL 553736 (Sept. 17, 2015).

[106] *E.g., CFTC v. McDonnell*, 287 F. Supp. 3d 213, 228 (E.D.N.Y. 2018).

[107] *United States v. Hayes et al.*, No. 20-cr-500, 2022 WL 597180, at *4 (S.D.N.Y. Feb. 28, 2022).

[108] In the past four years, the CFTC has brought over 30 cases involving some sort of fraud connected with digital assets. *E.g.*, Press Release, *CFTC Charges Four Operators for $44 Million Bitcoin Ponzi and Misappropriation Schemes*, CFTC (March 8, 2022), https://www.cftc.gov/PressRoom/PressReleases/8498-22. The majority of those actions involve fraudulent activity in the spot markets. Entities and individuals who solicit retail customers to trade digital assets may use online chat, gaming, and dating applications to connect with potential customers. Frequently, they also use websites to market and "offer" trading, often employing names that closely resemble CFTC registrants or other legitimate entities to cloak themselves in the indicia of reliability. Separately, digital assets, including bitcoin and other cryptocurrencies, are often used as a form of payment to fund fraudulent enterprises, including those involving more traditional financial products such as binary options, forex, and other commodities.

[109] *E.g.*, Press Release, *CFTC Orders Bitcoin Exchange Bitfinex to Pay $75,000 for Offering Illegal Off-Exchange Financed Retail Commodity Transactions and Failing to Register as a Futures Commission Merchant*, CFTC (June 2, 2016), https://www.cftc.gov/PressRoom/PressReleases/7380-16.

[110] *E.g.*, Press Release, *CFTC Sanctions Two Firms Offering Digital Asset-Based Swaps for Illegal Off-Exchange Trading and Registration Violations*, CFTC (July 13, 2020), https://www.cftc.gov/PressRoom/PressReleases/8201-20.

[111] *E.g.*, Press Release, *CFTC Orders Tether and Bitfinex to Pay Fines Totaling $42.5 Million*, CFTC (Oct. 15, 2021), https://www.cftc.gov/PressRoom/PressReleases/8450-21.

[112] Press Release, *CFTC Orders Coinbase Inc. to Pay $6.5 Million for False, Misleading, or Inaccurate Reporting and Wash Trading*, CFTC (March 19, 2021), https://www.cftc.gov/PressRoom/PressReleases/8369-21.

[113] The SEC brought parallel charges against McAfee and Watson relating to this conduct. Press Release, *SEC Charges John McAfee With Fraudulently Touting ICOs*, SEC (Oct. 5, 2020), https://www.sec.gov/news/press-release/2020-246.

[114] Press Release, *CFTC Imposes A $1.25 Million Penalty against Kraken for Offering Illegal Off-Exchange Digital Asset Trading and Failing to Register as Required*, CFTC (Sept. 28, 2021), https://www.cftc.gov/PressRoom/PressReleases/8433-21.

[115] Press Release, *CFTC Orders Event-Based Binary Options Markets Operator to Pay $1.4 Million Penalty*, CFTC (Jan. 3, 2022), https://www.cftc.gov/PressRoom/PressReleases/8478-22.

[116] Press Release, *Founders Of Cryptocurrency Exchange Plead Guilty To Bank Secrecy Act Violations*, U.S. Dep't of Justice (Feb. 24, 2022), https://www.justice.gov/usao-sdny/pr/founders-cryptocurrency-exchange-plead-guilty-bank-secrecy-act-violations.

[117] Press Release, *FinCEN Announces $100 Million Enforcement Action Against Unregistered Futures Commission Merchant BitMEX for Willful Violations of the Bank Secrecy Act*, U.S. Dep't of Treasury, Fin. Crimes Enf't Network (Aug. 10, 2021), https://www.fincen.gov/news/news-releases/fincen-announces-100-million-enforcement-action-against-unregistered-futures.

[118] Press Release, *Federal Court Orders BitMEX to Pay $100 Million for Illegally Operating a Cryptocurrency Trading Platform and Anti-Money Laundering Violations*, CFTC (Aug. 10, 2021), https://www.cftc.gov/PressRoom/PressReleases/8412-21.

[119] OCC 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* (Nov. 2021), https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2021/int1179.pdf.

[120] FDIC Financial Institution Letter 16-2022, Notification of Engaging in Crypto-Related Activities (Apr. 7, 2022), https://www.fdic.gov/news/financial-institution-letters/2022/fil22016.html.

[121] *See In re Anchorage Digital Bank, Nat'l Ass'n*, AA-ENF-2022-7 (Apr. 21, 2022), https://www.occ.gov/static/enforcement-actions/ea2022-010.pdf; Press Release, *FDIC and Federal Reserve Board issue letter demanding Voyager Digital cease and desist from making false or misleading representations of deposit insurance status*, FRB and FDIC (July 28, 2022), https://www.federalreserve.gov/newsevents/pressreleases/bcreg20220728a.htm.

[122] 15 U.S.C. § 45.

[123] 15 U.S.C. §§ 1693 *et seq*.

[124] 15 U.S.C. §§ 1691 *et seq*.

[125] Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in relevant part primarily at 15 U.S.C. §§ 6801-6809, §§ 6821-6827).

[126] Press Release, *At FTC's Request, Court Halts Bogus Bitcoin Mining Operation*, Fed. Trade Comm'n (Sept. 23, 2014), https://www.ftc.gov/news-events/news/press-releases/2014/09/ftcs-request-court-halts-bogus-bitcoin-mining-operation; *see also* Press Release, *Operators of Bitcoin Mining Operation Butterfly Labs Agree to Settle FTC Charges They Deceived Customers*, Fed. Trade Comm'n (Feb. 18, 2016), https://www.ftc.gov/news-events/news/press-releases/2016/02/operators-bitcoin-mining-operation-butterfly-labs-agree-settle-ftc-charges-they-deceived-consumers.

[127] *See, e.g.*, Emma Fletcher, *Reports Show Scammers Cashing in on Crypto Craze*, Fed. Trade Comm'n (June 2022), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze; *What to Know About Cryptocurrency and Scams*, Fed. Trade Comm'n (May 2022), https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams.

[128] *See, e.g.*, Fed. Trade Comm'n, Decrypting Cryptocurrency Scams Event (June 25, 2018), https://www.ftc.gov/news-events/events/2018/06/decrypting-cryptocurrency-scams).

[129] 12 U.S.C. § 5491; 12 U.S.C. § 5511.

[130] 12 U.S.C. § 5481(12), (14); 12 U.S.C.§ 5531(a); 12 U.S.C.§ 5536(a).

[131] Circulars are statements of policy that provide background information about applicable law, articulate considerations relevant to the CFPB's exercise of its authorities, and advise parties with authority to enforce federal consumer financial law. *See, e.g.,* Consumer Fin. Prot. Bureau, Consumer Financial Protection Circular 2022-02: Deceptive Representations Involving the FDIC's Name or Logo or Deposit Insurance (2022) (stating that "service providers likely violate the [Dodd-Frank Act's] prohibition on deception if they misuse the name or logo of the FDIC or engage in false advertising or make misrepresentations to consumers about deposit insurance" and recognizing this as particularly problematic with the emergence of financial technologies like digital assets), https://www.consumerfinance.gov/compliance/circulars/circular-2022-02-deception-representations-involving-the-fdics-name-or-logo-or-deposit-insurance/.

[132] The CFPB Consumer Complaint Database allows interested parties to search public complaints to identify those complaints specifically referencing digital assets. *See* Consumer Complaint Database, https://www.consumerfinance.gov/data-research/consumer-complaints/search. To search all complaints, filter by product: "money transfer," "virtual currency," or "money service" and sub-product: "virtual currency." For complaints received since April 2017, filter by product: "virtual currency."

[133] *See* Press Release, *FinCEN Recognizes Law Enforcement Cases Significantly Impacted by Bank Secrecy Act Filings*, U.S. Dep't of Treasury, Fin. Crimes Enf't Network (May 19, 2020), (highlighting FinCEN Director's Law Enforcement Award in Transnational Security Threat category). https://www.fincen.gov/news/news-releases/fincen-recognizes-law-enforcement-cases-significantly-impacted-bank-secrecy-act.

[134] Press Release, *FinCEN Launches "FinCEN Exchange" to Enhance Public-Private Information Sharing*, U.S. Dep't of Treasury, Fin. Crimes Enf't Network (Dec. 4, 2017), https://www.fincen.gov/news/news-releases/fincen-launches-fincen-exchange-enhance-public-private-information-sharing.

[135] U.S. Dep't of Treasury, Fin. Crimes Enf't Network, FinCEN Exchange Questions and Answers, https://www.fincen.gov/resources/fincen-exchange/fincen-exchange-frequently-asked-questions; U.S. Dep't of Treasury, Fin. Crimes Enf't Network, FinCEN Exchange, https://www.fincen.gov/resources/financial-crime-enforcement-network-exchange.

[136] U.S. Dep't of Treasury, Fin. Crimes Enf't Network, FinCEN Exchange, *supra* note 135.

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

[138] *See* 18 U.S.C. § 1510(b); 12 U.S.C. § 3420(b).

[139] *See* 18 U.S.C. § 20 (defining "financial institution" "as used in this title"); 12 U.S.C. § 3401 (defining "financial institution" "[f]or the purpose of this chapter").

[140] 31 U.S.C. § 5312(a)(2).

[141] From the consultations undertaken in preparing this Report, the Department understands that regulatory agencies that issue subpoenas to VASPs and other entities in the digital assets industry have faced similar issues concerning potential disclosures by those entities to customers when their records are sought via subpoena. It may therefore be appropriate to consider whether any proposed legislative action on anti-tip-off provisions should extend to administrative subpoenas issued by regulators such as the SEC and CFTC.

[142] Measures to strengthen the federal registration prong of § 1960 (18 U.S.C. § 1960(b)(1)(B)) are likely to be especially important if states heed industry calls to exempt certain cryptocurrency transactions from the requirements of state money transmission laws—which could have the effect of removing those transactions from the reach of § 1960(b)(1)(A) (defining an "unlicensed money transmitting business" to include an entity that "is operated without an appropriate money transmitting license in a State where such operation is punishable as a misdemeanor or a felony under State law"). *See* Eric Lipton & David Yaffe-Bellany, *Crypto Industry Helps Write, and Pass, Its Own Agenda in State Capitols*, N.Y. Times (Apr. 10, 2022), https://www.nytimes.com/2022/04/10/us/politics/crypto-industry-states-legislation.html.

[143] *Compare* 18 U.S.C. §§ 1343, 1344 (statutory maximum terms of imprisonment of 20 and 30 years for wire and bank fraud offenses), *and* 18 U.S.C. § 1956 (statutory maximum terms of imprisonment of 20 years for money laundering), *with* 18 U.S.C. § 1957 (statutory maximum terms of imprisonment of 10 years for engaging in monetary transactions in property derived from specified unlawful activity).

[144] *See* U.S.S.G. §§ 2S.1(a)(2), 2S1.3(a)(2) (advisory Guidelines applicable to § 1960 offenses calculated based on amount of funds laundered or transferred).

[145] 18 U.S.C. § 3571(b)(3), (c)(3), (d).

[146] *See, e.g.*, 18 U.S.C. § 1956(a)(1)-(2).

[147] Existing law provides enhanced penalties for aggravated violations of the BSA, *see* 31 U.S.C. § 5322(b), and officials have previously acknowledged the potential utility of similar penalties for crimes relating to digital assets. *See* Letter from Charles P. Rettig, Comm'r, Internal Revenue Serv., to Sen. Margaret Wood Hassan, at 2 (Dec. 21, 2021) (stating that "[e]nhancements to" certain civil penalties and to the "criminal penalties" in § 1960 "for egregious behavior in the cryptocurrency space could also be applied to promote voluntary compliance"), https://www.hassan.senate.gov/imo/media/doc/crypto.pdf.

[148] 18 U.S.C. § 1960(b)(1)(B).

[149] *See generally* U.S. Dep't of Treasury, Fin. Crimes Enf't Network, FIN-2019-G001, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, *supra* note 5.

[150] *See, e.g.*, *United States v. Dimitrov*, 546 F.3d 409, 413 (7th Cir. 2008); *United States v. Keleta*, 441 F. Supp. 2d 1, 3 (D.D.C. 2006).

[151] Of note, Congress recently expanded to 10 years the limitations period applicable to disgorgement claims brought by the SEC for violations of the anti-fraud provisions of the securities laws. *See* National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, Title LXV, § 6501(a), 134 Stat. 4626 (2021).

[152] *See 2020 Cryptocurrency Enforcement Framework*, *supra* note 2, at 50.

[153] *See, e.g.*, *United States v. Reed*, No. 20-cr-500, 2022 WL 597180, at *4 (S.D.N.Y. Feb. 28, 2022) (joining other courts in holding that "under the plain language of the [relevant statute], cryptocurrencies fall within the definition of commodities").

[154] By contrast, forfeiture for securities violations charged under 18 U.S.C. § 1348 is currently authorized under 18 U.S.C. § 981(a)(1)(C), which authorizes forfeiture of proceeds of "specified unlawful activity." As defined under 18 U.S.C. §§ 1956(c)(7) & 1961(1)(D), specified unlawful activity includes "fraud in the sale of *securities*" (emphasis added), but there is no corresponding clause for commodities fraud.

[155] *See* 19 U.S.C. § 1607 (administrative forfeiture under the customs laws); 18 U.S.C. § 981(d) (making customs-law regime applicable to items seized for civil forfeiture).

[156] *See* Asset Forfeiture Policy Manual (2021), Chap.5, Sec.II.A.

[157] 19 U.S.C. § 1607(a)(1), (4).

[158] Pub. L. No. 116-283, 134 Stat. 4553 (2021).

[159] 31 U.S.C. § 5322(a).

[160] *Id*. § 5322(b).

[161] U.S.S.G. §§ 2S1.1(a)(2), 2S1.3(a)(2); *see United States v. Braxtonbrown-Smith*, 278 F.3d 1348, 1356 (D.C. Cir. 2002) ("'Section 2S1.1 measures the harm to society that the money laundering causes to law enforcement's efforts to detect the use and production of ill-gotten gains.'") (quoting *United States v. Allen*, 76 F.3d 1348, 1369 (5th Cir. 1996)).

[162] *Cf*. U.S.S.G. § 2S1.3(a)(2), § 2S1.3 cmt. n.1.

[163] *See* Threshold for the Requirement To Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds That Begin or End Outside the United States, and Clarification of the Requirement To Collect, Retain, and Transmit Information on Transactions Involving Convertible Virtual Currencies and Digital Assets With Legal Tender Status, 85 Fed. Reg. 68005 (proposed Oct. 27, 2020) (to be codified at 31 C.F.R. pts. 1010, 1020).

[164] *See id*. at 68010.

[165] U.S. Dep't of Treasury, Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art, *supra* note 26, at 26.

[166] *Id*. at 26-27.

[167] *See, e.g*., 31 U.S.C. § 5312(a)(2)(J), (R); 31 C.F.R. § 1010.100(ff)(5)(i)(A).

[168] U.S. Dep't of Justice, Comprehensive Cyber Review, *supra* note 55, at 62-65.