U.S. Department of Justice
Washington, DC

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

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

June 6, 2022

Dear Mr. President,

I am pleased to submit to you the attached Report pursuant to Section 8(b)(iv) of your March 9, 2022, *Executive Order on Ensuring Responsible Development of Digital Assets*.

As your Executive Order notes, the growing use of digital assets in the global financial system has profound implications for investors, consumers, and businesses and increases the risk of crimes such as money laundering, ransomware, terrorist financing, fraud and theft, and sanctions evasion. Strong international law enforcement cooperation will be essential to best position the United States and its partners to detect, investigate, prosecute, and otherwise disrupt criminal activity related to digital assets, and to overcome the unique obstacles posed by the features of these technologies to law enforcement efforts to combat their misuse.

In response to your Executive Order, the Department of Justice engaged in a collaborative effort with the Department of State, Department of the Treasury, Department of Homeland Security, Securities and Exchange Commission, and Commodity Futures Trading Commission to determine how to best strengthen international law enforcement cooperation. As this Report explains in more detail, the Department of Justice and our law enforcement and regulatory partners have already taken steps to combat the illicit use of digital assets, but efforts must evolve to meet the challenge. The Report recommends expanding our operational and capacity building efforts with international partners; increasing information sharing, coordination, and deconfliction; and closing regulatory gaps across jurisdictions.

I look forward to working with our interagency partners on this important issue.

Respectfully,

Merrick B. Garland
Attorney General

cc: Mr. Antony Blinken, Secretary of State
Ms. Janet Yellen, Secretary of the Treasury
Mr. Alejandro Mayorkas, Secretary of Homeland Security
Mr. Gary Gensler, Chair of the Securities and Exchange Commission
Mr. Rostin Behnam, Chairman 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 "the Executive Order"). Section 8(b)(iv) of the Executive Order directed the Attorney General to submit a report on how to strengthen international law enforcement cooperation for detecting, investigating, and prosecuting criminal activity related to digital assets. The Attorney General now issues that Report, in an effort led by the Department of Justice's National Cryptocurrency Enforcement Team, in consultation with the Secretary of State (State), the Secretary of the Treasury (Treasury), and the Secretary of Homeland Security (DHS), and with input from the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC).

The United States supports the responsible use and development of digital assets. This Report focuses on the criminal misuse of digital assets,[1] the most common of which are cryptocurrencies.[2] The perceived pseudonymity of cryptocurrencies makes them attractive vehicles for money laundering and other criminal exploits, and their widespread promotion as investment vehicles has led to opportunities for criminals to target consumers and retail investors—particularly those who seek to profit from investing in this emerging financial ecosystem, but are unfamiliar with the technology and the attendant risks of the market. Criminal actors leverage the innovation, claims of decentralization, and anonymizing features of cryptocurrencies to facilitate criminal conduct in all corners of the world. The cross-border nature of digital asset technologies accordingly requires collaboration with foreign law enforcement partners to locate and gather electronic records and digital evidence involving off-shore digital asset issuers, trading platforms, service providers, and other online infrastructure; to seize and prevent further distribution of digital assets linked to crime; and to identify and hold responsible criminal actors who exploit pseudonymity features of the Internet and decentralized finance (DeFi) technologies to avoid detection and prosecution.

Cross-border collaboration is critical because uneven and often inadequate regulation and supervision, coupled with a lack of compliance enforcement for digital asset trading platforms and other service providers, allow criminals to expose the U.S. and international financial systems to risk from jurisdictions where regulatory standards and enforcement are less robust.[3] Gaps in anti-money laundering and counter-financing-of-terrorism (AML/CFT) regulatory regimes across jurisdictions not only jeopardize the safety and stability of the international financial system, but also create opportunities for criminal actors to engage in "jurisdictional arbitrage" to take advantage of regulatory inconsistencies across jurisdictions, or in some cases, complete lack of regulation and supervision.

The Report begins by explaining the features of digital asset transactions that differentiate them from traditional financial transactions and how those features may affect transnational investigations. The Report then explains several ways in which U.S. law enforcement agencies and regulators have responded to the challenges posed by digital asset investigations. Although international cooperation has been crucial to overcome obstacles in numerous successful cases involving law enforcement efforts to combat the illicit use of digital assets (several examples of which are detailed in Annex B to this Report), there remain significant challenges to fully leveraging

mutual legal assistance between the United States and its foreign law enforcement partners to bring criminal actors who misuse digital assets to justice, and to seize their criminal proceeds so as to deprive criminal actors of their ill-gotten profits and to provide restitution to victims. The Report concludes with recommendations to bolster enforcement and improve international cooperation by (1) undertaking additional efforts to build the capacity of foreign counterparts to conduct the type of complex and highly specialized investigations required in this area; (2) engaging in robust information sharing, early coordination, and deconfliction in investigations across various domestic and international agencies; and (3) promoting more uniform regulation among the U.S. and foreign partners in the digital assets space through implementation of international standards that could help reduce the risks posed by jurisdictional arbitrage. Implementation of effective AML/CFT safeguards, in line with international standards, are among the recommended actions to support law enforcement's ability to identify criminal actors who exploit digital asset technology.

In addition, the Report includes the following Annexes:

Annex A provides additional information on the various types of criminal activity that are facilitated through the illicit use of digital assets.

Annex B provides multiple examples in which cooperation between U.S. law enforcement agencies and their foreign counterparts was integral to the success of cross-border investigations involving digital assets.

Annex C describes recent international training efforts conducted by federal law enforcement agencies and regulators with expertise in digital asset investigations—i.e., the Department of Justice (including the Federal Bureau of Investigation (FBI) and the Drug Enforcement Administration (DEA)); the Department of Homeland Security (DHS) (including Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and U.S. Secret Service (USSS)); the Department of the Treasury (Treasury) (including the Financial Crimes Enforcement Network (FinCEN), the Office of Foreign Assets Control (OFAC), and the Internal Revenue Service-Criminal Investigation Division (IRS-CI)); the Securities and Exchange Commission (SEC), and the Commodity Futures Trading Commission (CFTC). The Department of State provides support for many of these efforts.

II. CHALLENGES ARISING IN THE INTERNATIONAL INVESTIGATION OF CRIMES RELATED TO DIGITAL ASSETS

The United States has an interest in supporting responsible financial innovation, expanding access to safe and affordable financial services, and reducing the cost of domestic and cross-border funds transfers and payments, including through the continued modernization of public payment systems. Although cryptocurrencies and other digital assets have lawful and legitimate uses, criminals seek to exploit certain characteristics and features of these technologies to commit and profit from a variety of crimes.[4] As the Executive Order also noted, digital assets are used in a variety of ways to facilitate thefts, frauds, and abuses that target victims in the United States and abroad.[5] For example, criminal actors rely on digital assets to extort ransomware payments from victim companies; dark web traffickers use digital assets to buy and sell drugs, malware and other hacking tools, weapons, and other contraband; money launderers use digital assets to hide criminal proceeds and the identities of those who profit from them; and nation states and terrorist groups exploit digital assets to circumvent U.S. and international sanctions regimes.[6]

Because many of these crimes—and the digital asset financial infrastructure itself—transcend international borders, efforts to combat the criminal abuse of digital assets necessitate an international approach. As explained below in Section II.A, several of the features that make digital assets an attractive vehicle for perpetrating and profiting from crime can also affect how those crimes are investigated at an international level.

A. Digital Asset Transactions Have Distinct Characteristics That Can Both Enhance and Hamper Investigative Efforts

Digital assets can be used to store and transfer value in a manner similar to traditional financial systems. Transactions involving digital assets, however, differ from traditional financial transactions in several fundamental respects that are relevant to the way in which the United States should approach international cooperation efforts.[7] Those differences include:

Immutability: Transactions involving cryptocurrencies are, in most cases, quickly verified and permanently recorded on distributed ledgers publicly available on the Internet. The ability to trace a financial transaction through a public ledger enhances law enforcement's ability to follow the money in ways that are not possible with traditional financial systems that use non-public accounts and business records. This has the potential to enhance law enforcement's ability to detect suspicious criminal activity, generate leads to further investigations, and provide a permanent record for use in an eventual prosecution.

Transactions Involving Cryptocurrencies Can Occur Without Regard to Geographic Borders: Several features of distributed ledger technologies ensure that transactions involving digital assets can be made without regard to geographic location. To begin, any transfer of digital assets can occur regardless of the location of those seeking to initiate the transaction. That is because the only requirement for transmitting

the contents of, or value associated with, a particular wallet is the use of a private key (which functions like a password or a PIN). These transactions, moreover, do not require the use of any intermediary; rather, upon initiation of a blockchain-based request, the transmission is broadcast over the Internet to a series of nodes around the world. The request functions through any Internet-capable connection, regardless of geographic borders. Such characteristics have allowed for the widespread adoption and growth of the digital asset industry. Criminal actors connected to the Internet from anywhere in the world can also exploit these characteristics to facilitate large-scale, nearly instantaneous cross-border transactions without traditional financial intermediaries that have AML/CFT programs.

Pseudonymity: Many digital asset transactions are pseudonymous. Certain cryptocurrencies, such as bitcoin,[8] operate their ledgers using "addresses," or long strings of alphanumeric characters. Although the ledgers do not contain names or traditional account identifiers associated with any particular address, the users of the addresses may potentially be identified by analyzing the transactions between those addresses and other entities. While cryptocurrency transactions do not require an intermediary, criminals using digital assets often transact with businesses and infrastructure providers, such as virtual asset service providers (VASPs),[9] in furtherance of their activities. Those organizations, depending upon the jurisdiction, have AML/CFT obligations that often require verification of customer identity and other financial account information. For instance, illicit actors often transfer cryptocurrency to companies that offer to exchange cryptocurrencies for fiat currency or other digital assets, colloquially known as "exchanges" (which are also VASPs). In instances where exchanges collect information, such as through "Know Your Customer" (KYC) and other AML/CFT policies that are legally required in the United States and other jurisdictions, law enforcement may be able to connect illicit transactions with real-world identities by using "blockchain analytics." That is, investigators may be able to identify users by analyzing digital asset transactions on a publicly viewable blockchain and combining such information with other non-public information gathered through appropriate legal process and international law enforcement cooperation.

Anonymity: Some digital asset transactions are designed for anonymity. For instance, Anonymity Enhanced Cryptocurrencies (AECs) are designed to obscure the links between wallet addresses, such that blockchain analytics are not able to reliably connect multiple transactions. AECs use obscured blockchains that limit or eliminate the traceability of those assets. Use of AECs, combined with a lack of adequate AML/CFT policy implementation by VASPs, help criminals hide the movement or origin of funds, creating additional obstacles for investigators.

Obfuscation Tools: Criminal actors may take additional steps designed to anonymize cryptocurrency transactions on several blockchains by using a series of obfuscation tools. Among other techniques, illicit actors may (1) use a "mixer" or "tumbler"—i.e., software services that mix otherwise traceable cryptocurrency with other funds, frequently including funds received from other customers, before sending it to the requested recipient address; (2) engage in "chain hopping," which involves the rapid swapping of one cryptocurrency for another; and (3) engage in "off-chain transactions," which involves the transfer of private keys from one person to another without recording the transaction on the blockchain.

Unhosted Wallets: Criminal actors may use "unhosted wallets" to shift large sums of money quickly and covertly across the globe to support

their illegal activities. Unhosted (or non-custodial) wallets are digital storage mediums that are not hosted by a third-party institution, such as a VASP, but rather are held by individual digital asset owners who maintain possession of their own private keys, which presents challenges to law enforcement's capability to restrain or seize assets. A significant portion of the world's digital assets is held in unhosted wallets.

B. The Nature of Transactions Involving Digital Assets Poses Several Obstacles to the Investigation of Criminal Activity Involving Their Use

Crimes involving digital assets are subject to the same challenges and constraints that affect many cross-border criminal investigations. U.S. investigators and regulators, however, have encountered a recurring set of challenges attributable to the unique features of cryptocurrency and other digital assets described above.

1) The speed and cross-border nature of digital asset transactions poses challenges to the timely collection of evidence and the effectuation of restraints and seizures of assets.

Transactions involving cryptocurrency and other digital assets are often fast-moving. Criminal actors using these technologies can victimize targets quickly, move funds nearly instantaneously and (often) irreversibly, and take steps to ensure that electronic records and digital evidence not on the blockchain concerning their activities (such as servers and communications used in furtherance of their crimes) are quickly deleted, inhibiting investigations. To effectively combat crime involving cryptocurrency and other digital assets, law enforcement must be able to rapidly obtain evidence concerning the crimes under investigation and the transactions involved. Many VASPs and other companies from which law enforcement seeks records operate abroad, and that can impede law enforcement's ability to obtain evidence, for several reasons.

First, the process of obtaining records from VASPs and other companies operating abroad can be slow. This is particularly true where an entity's country of operation has laws limiting U.S. law enforcement's ability to obtain records from the entity directly through voluntary means or via informal law enforcement channels. Law enforcement may also seek assistance through formal channels, either pursuant to a bilateral mutual legal assistance (MLA) treaty, MLA measures in a multilateral treaty such as the United Nations Convention on Transnational Organized Crime or the Convention on Cybercrime of the Council of Europe (commonly known as the Budapest Convention),[10] or in the event no treaty mechanism exists, through letters rogatory, foreign domestic law mechanisms, and/or comity and reciprocity.[11] These formal requests submitted government-to-government can be used to obtain the production of evidence located abroad, but may sometimes take months, or even years, to execute. The time required for execution varies by country and may be affected by the volume of requests submitted to that country, the complexity of the request, or the government's familiarity with the technologies involved, among other factors. As a result, while MLA requests and other processes are critical (and often the only available) evidence-gathering tools, they can sometimes be too slow for effective investigation in cybercrime and cryptocurrency-related matters where swift action is imperative.

Second, it may not always be possible to obtain the preservation of the requested records while attempts to obtain these records through MLA requests or other processes are pending.

Although rapid preservation of the records of various electronic and internet service providers can be obtained through treaty-based and informal networks of law enforcement agencies, including the "24-7 Network," these networks often do not include preservation requests for VASPs.

Third, such records may not always be available. Many countries in which VASPs operate have differing standards regarding records retention, data privacy, and AML/CFT requirements that may limit the scope of evidence available for collection. Additionally, VASPs and other companies may lack the ability to prevent disclosure to accountholders, leaving law enforcement with the unfortunate choice between foregoing important evidence or risking disclosure of a sensitive investigation to its target, which could lead to the destruction of evidence, efforts to avoid prosecution through flight, or other risks to law enforcement's capability to investigate, prosecute, and otherwise disrupt the criminal activity.

Fourth, and compounding each of the challenges referenced above, many VASPs and other companies have attempted to structure their business using more "decentralized" or distributed architectures, such as registering in one country, having personnel located in other countries, and hosting technical infrastructure and/or private keys in separate countries. Such architectures pose a significant investigative burden for law enforcement to identify the proper entity to approach with requests for information, or the proper country to send a formal or informal request for assistance. At times, despite extensive and good-faith efforts to do so, law enforcement belatedly learns that a company served with legal process via an MLA request, or the country seeking to execute that MLA request, cannot do so because the company's records (or personnel) are located (or have been moved) elsewhere. This international goose-chase may be intended to, and sometimes does, stall criminal investigations.

Finally, distributed business infrastructures can result in a single company being subject to multiple competing domestic legal obligations. Navigating these conflicts and complex questions of law can slow the production of records or, in some instances, halt their production entirely.

All these challenges pose similar obstacles to law enforcement's capability to restrain and seize digital assets in instances where law enforcement can identify illicit digital assets held in "hosted wallets," or custodial wallets maintained by third parties such as VASPs. In general, it may be difficult for law enforcement to serve a seizure order or a request to seize assets upon a foreign entity and obtain its enforcement if, for example, the entity is in a jurisdiction with which the United States lacks a treaty relationship, or if that jurisdiction is unable or unwilling to assist through other means. Certain foreign VASPs may pose additional challenges to effectuating seizure orders, for instance, if the exchange is headquartered in one jurisdiction but maintains personnel or records elsewhere; the exchange intentionally obfuscates its place of operation; or the exchange is unable to effectuate a seizure order because it lacks control over the private keys needed to transfer the funds. Accordingly, U.S. law enforcement's ability to restrain and seize assets involving a hosted wallet varies greatly depending upon the VASP at issue and the jurisdiction(s) in which it operates.

2) Foreign law enforcement partners' ability and willingness to assist U.S. investigations of crimes involving digital assets may depend on the foreign jurisdiction's authorities and how they categorize digital asset issuers, trading platforms, and other VASPs.

Differences in the substantive treatment or regulation of digital assets across legal systems—and limitations on or a lack of governmental authorities in some countries—may complicate the ability or willingness of foreign partners to assist in U.S. investigations. For instance, many countries have not fully implemented the global AML/CFT standards to digital assets, as set forth by the Recommendations of the Financial Action Task Force (FATF), an inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing, and the financing of proliferation of weapons of mass destruction, of which the United States was a founding member. In parallel, regulators across jurisdictions are grappling with the categorization of new digital asset products and many are currently deciding what, if any, regulatory requirements to attribute to digital asset issuers, trading platforms, and other VASPs. In addition, not all foreign countries have asset-seizure authority outside of criminal prosecutions analogous to civil-forfeiture authorities under U.S. law—authorities that U.S. law enforcement agencies have regularly marshaled in the cryptocurrency sphere. At the same time, foreign financial regulators uncertain of their authority over certain classes of digital assets may be less willing, or believe themselves less able, to supply information or take measures requested by their U.S. counterparts.

3) Some foreign partners are still developing the tools and training required for effective investigation of crimes involving digital assets.

The skills and expertise necessary to conduct thorough and complex investigations involving digital assets remain highly specialized. Digital asset technology is still new enough that many countries are in the beginning stages of training their administrative and law enforcement agencies on the use of the technology and how to investigate and prosecute related crimes. In many instances, prosecutors and investigators have had only limited exposure to digital assets in their investigations and face a steep learning curve due to the perceived technical complexity of digital assets and their relatively recent adoption. Although some foreign law enforcement agencies are quite advanced in their ability to investigate crimes involving digital assets, most face challenges due to limited resources dedicated to conducting ordinary money laundering and other financial investigations, let alone complex investigations involving digital assets that require specialized tools and technical expertise.

In addition, as criminal actors in the digital asset space have grown more sophisticated, so too have blockchain analytics tools and other proprietary technologies used to further investigations. Although those tools remain important in the detection and investigation of criminal activity, many of them are costly and outside the financial reach of some jurisdictions. At the same time, investigators in those countries may not be well-versed in publicly available or open-source blockchain analytics tools that are available as a low-cost or free alternative to proprietary technologies.

4) Effective sharing of information relating to investigations involving digital assets is critical to deconfliction efforts and preservation of resources.

The transnational nature of criminal schemes involving digital assets creates a significant likelihood that law enforcement agencies in multiple countries will end up investigating the same illicit conduct. When multiple U.S. agencies have concurrent jurisdiction to investigate a crime, the United States has found that close and early coordination is often crucial to furthering its investigations—both to ensure that information is shared early to harness potential opportunities for essential investigative steps, and to avoid duplicative efforts that waste investigative resources and erode relationships with public and private sector partners. Similar coordination and deconfliction is equally vital among U.S. law enforcement agencies and foreign law enforcement partners, who may be targeting the same transnational criminal syndicates and have useful intelligence regarding the same threat actors who abuse legitimate digital and financial infrastructure to perpetrate their crimes. Nevertheless, deconfliction across different types of criminal investigations may be difficult across international law enforcement agencies in situations in which individual agencies have different reporting formats or structures, or do not have robust systems that facilitate comprehensive or accurate searches for investigatory information.

C. U.S. Law Enforcement and Regulatory Agencies Have Taken Steps to Address These Challenges

The Department of Justice is actively engaging with its foreign counterparts to address the challenges described above. Among other things, the Department of Justice has undertaken efforts to better understand other countries' domestic laws regarding evidence collection related to VASPs and other entities from which law enforcement seeks records in cybercrime and digital assets-related investigations, and to increase its familiarity with the unique needs presented in those investigations. Additionally, the Department of Justice is actively engaged in the promotion of the Budapest Convention and its Second Additional Protocol, which the United States signed upon its opening for signature on May 12, 2022. The Second Additional Protocol aims to further enhance cooperation on cybercrime and electronic evidence-sharing through more efficient mutual assistance processes and other forms of cooperation between countries, including obtaining information in emergencies and direct cooperation between law enforcement in one country and electronic communication service and remote computing service providers and other private entities in another country. Efforts like these to strengthen international cooperation mechanisms and the efficiency of processes for evidence sharing should further investigations involving digital assets.

Additional steps U.S. law enforcement agencies and regulators have taken to address the challenges posed by cross-border investigations involving digital assets include the following: (1) developing expertise that can be shared with foreign counterparts; (2) working through international standard-setting organizations to support uniform regulation of actors in the digital asset space and facilitate information-sharing among law enforcement and regulators; and (3) using a variety of tools and authorities across government to respond to the growing and evolving threat posed by malicious actors exploiting digital assets.

Several examples of successful cases involving law enforcement efforts to combat the illicit use of digital assets are detailed in Annex B to this Report.

1) Development and sharing of expertise with foreign counterparts.

U.S. law enforcement agencies have undertaken several key initiatives designed to harness their own expertise in digital asset-related investigations and facilitate the sharing of that expertise with foreign counterparts through training and case-specific contacts. Within the Department of Justice, for example, the Financial Crimes Section of the FBI established the Virtual Assets Unit (VAU) in February 2022. The VAU serves as a nerve center for the FBI's digital asset efforts, in which digital asset experts and cross-divisional resources are embedded in a task force setting to seamlessly integrate intelligence and operations across the FBI. The VAU will provide training, equipment, and field-deployed expertise in blockchain analysis and digital asset seizure, as well as an innovation team dedicated to remaining ahead of threats posed by rapidly emerging technologies.

The VAU works closely with the Department of Justice's National Cryptocurrency Enforcement Team (NCET), which was created in October 2021 to investigate and support complex prosecutions of criminal misuses of cryptocurrency, particularly crimes committed by digital asset exchanges, mixing and tumbling services, and money laundering infrastructure actors. Housed within the Criminal Division, the NCET combines the expertise of the Money Laundering and Asset Recovery Section (MLARS), Computer Crime and Intellectual Property Section (CCIPS), and other Department litigating components, including experts detailed from U.S. Attorneys' offices across the country.

The NCET and VAU are contributors to the Department of Justice's International Virtual Currency Initiative,[12] which works to strengthen international cooperation and capacity building with respect to the illicit use of cryptocurrency. That Initiative operates in part through the U.S. Transnational and High Tech Crime Global Law Enforcement Network (GLEN), an initiative funded by the Department of State's Bureau of International Narcotics and Law Enforcement Affairs and managed in partnership with the Department of Justice. The GLEN features the Department of Justice's International Computer Hacking and Intellectual Property (ICHIP) Attorney Advisors, who are located across the world and include a dedicated subject-matter expert ICHIP for Dark Web and Cryptocurrency.[13] These GLEN capacity-building initiatives feature ICHIP leadership in three regional Cryptocurrency Working Groups (Southeast Asia, Eastern Europe, and Latin America) and provide country-focused assistance to judges, prosecutors, investigators, and forensic analysts. Additionally, Resident Legal Advisors (RLAs) funded by the Department of State's Bureau of Counterterrorism have addressed terrorists' use of virtual currencies in their capacity-building programs.

These are not the only international training efforts conducted by federal law enforcement agencies and regulators with expertise in cryptocurrency investigations. In recent years, trainings have been conducted by the Department of Justice, including the FBI, the DEA, and the National Security Division; DHS, including HSI and USSS; Treasury, including FinCEN and IRS-CI; the SEC; and the CFTC. Annex C provides additional examples of, and information about, these training and capacity-building efforts.

The United States is by no means alone in its efforts to combat digital asset crime and share its knowledge of such investigations with others. For example, Europol and its European Cybercrime Centre (EC3) have published a variety of guides for digital currency investigations, including

guides for Ethereum and Bitcoin, two of the most prevalent types of digital assets; and points of contact for digital-asset-related records. Additionally, many U.S. law enforcement agencies have embedded liaisons who work with Europol at The Hague and in other locations around the world to help facilitate information sharing and collaboration with foreign law enforcement partners. These liaisons often assist with digital asset investigations, thereby providing their partners with on-the-job capacity building.

2) Participation in international standard-setting fora.

In addition to the multiple efforts to facilitate international evidence collection as detailed above (including the Budapest Convention and MLA requests), the United States is participating in several international fora designed to help address the cross-border challenges posed by digital assets and to mitigate risks of jurisdictional arbitrage. These include the following:

Financial Action Task Force (FATF): The United States—led by Treasury—and Japan co-chair the Virtual Assets Contact Group (VACG) at the FATF, which sets international standards for combating money laundering, terrorist financing, and other illicit finance that more than 200 countries and jurisdictions have committed to implement. Through its role as co-chair of the VACG, as well as individually, the United States is working with a range of countries to understand and overcome challenges to implementation of the FATF standards.

As recognized in Treasury's 2022 National Money Laundering Risk Assessment, uneven—and often inadequate—AML/CFT regulation and international supervision for virtual assets (a significant subset of digital assets) and VASPs allow criminals to engage in jurisdictional arbitrage and expose the U.S. financial system to risk from jurisdictions where regulatory standards and enforcement are less robust.[14] Since 2018, the FATF has made clear that its standards apply to virtual assets and VASPs, and that VASPs are subject to the same full set of obligations and are generally expected to carry out the same measures as other financial institutions. These include implementation of AML/CFT programs (including risk assessment, customer due diligence, record keeping, imposition of targeted financial sanctions, and filing of suspicious activity reports), as well as compliance with the "Travel Rule" (i.e., the application of the FATF's wire transfer requirements, found in Recommendation 16),[15] which requires VASPs to obtain, hold, and transmit required originator and beneficiary information, immediately and securely, when conducting digital asset transfers and retain accurate information about the parties to cryptocurrency transactions.[16] The FATF has published several resources to support countries and the private sector with implementation, including most recently an October 2021 updated version of its guidance on implementation, as well as non-public guidance to support law enforcement and other competent authorities with investigations related to criminal misuse of virtual assets.

International Organization of Securities Commissions (IOSCO): Two of the principal financial regulators in the United States—the SEC and CFTC—actively participate in digital-asset matters through IOSCO, a multilateral organization whose members regulate over 95% of the world's securities markets. SEC and CFTC staff contribute to workstreams on stablecoins (defined generally as cryptocurrencies with mechanisms that are aimed at maintaining a stable value, such as by pegging the value of a coin to a specific currency, asset, or pool of assets), "unbacked" crypto-assets (defined broadly to include all digital assets other than stablecoins

and tokenized assets), decentralized finance (DeFi, discussed further in Annex A), and, as to the CFTC, cryptocurrency derivative products. The purpose of those workstreams is to minimize the risks of jurisdictional arbitrage and market fragmentation, as well as to provide a forum to share information and experiences, including on regulatory proposals and emerging practices across jurisdictions. The SEC and CFTC also participate in enforcement cooperation-focused committees of IOSCO and are founding members of the Committee 4 (C4), which works to improve cross-border cooperation and knowledge-sharing in securities investigations and enforcement matters and is increasingly focused on digital assets. The SEC is the current chair of C4.

In addition, both the SEC and CFTC are signatories to IOSCO's 2002 Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (MMoU), and the 2016 Enhanced MMoU (EMMoU). These serve as frameworks for the transmission of materials and information relevant to specific investigations and enforcement matters. Both the SEC and the CFTC are active participants of the IOSCO group responsible for screening applications to the MMoU/EMMoU, and, in this capacity, may address specific technical-assistance questions raised by foreign counterparts. The MMoU covers the provision of bank, brokerage, and corporate and beneficial ownership records; the EMMoU additionally covers audit work papers, compelled testimony, asset freeze advice and information, non-content records of internet service providers, and telephone records. In recent years, more than 4,000 cooperation requests have been made annually by signatories of the MMoU and EMMoU, with the SEC in the top three users every year, and the CFTC in the top ten. Currently, the 2002 MMoU has 125 signatories and the 2016 Enhanced MMoU has 22 signatories.[17]

3) Other U.S. Government efforts to combat illicit use of digital assets.

U.S. law enforcement agencies have been coordinating and working closely with other departments and agencies in combating illicit digital asset use in a manner that recognizes the importance of a whole-of-government approach that ensures maximum disruptive impact against actors who criminally misuse digital assets. For instance, law enforcement has worked closely with OFAC, which has been active in the digital assets area by imposing sanctions on perpetrators of ransomware activities, who often make ransom demands in cryptocurrency; entities that facilitate the digital ransom payments; and more recently, nested cryptocurrency exchanges, a darknet market, and a mixer that was used by the Democratic People's Republic of Korea (DPRK) to support its malicious cyber activities and the laundering of stolen cryptocurrency.[18] OFAC has also taken actions against money launderers in receipt of stolen cryptocurrencies obtained through cyber intrusions linked to sanctioned actors. In 2021, OFAC published a sanctions compliance guidance for the cryptocurrency industry[19] and issued an updated advisory related to ransomware payments, which highlights the proactive steps companies can take to mitigate potential sanctions risks associated with ransomware payments, including actions that OFAC would consider to be "mitigating factors" in any related enforcement action.[20] Similarly, U.S. law enforcement has worked closely with members of the intelligence community, including U.S. Cyber Command and the National Security Agency, in disrupting and degrading an array of cybercriminal activity, ranging from ransomware actors to the threats posed by nation-state hackers who generate revenue through the theft of cryptocurrency.[21]

III. RECOMMENDATIONS TO IMPROVE INTERNATIONAL COOPERATION IN DETECTING, INVESTIGATING, AND PROSECUTING CRIMINAL ACTIVITY RELATED TO DIGITAL ASSETS

The United States has successfully worked with its foreign law enforcement partners to disrupt criminal organizations exploiting digital assets and bring these criminals to justice. However, additional steps can be taken to (1) strengthen U.S. agencies' existing operational and capacity-building initiatives; (2) deepen information sharing partnerships and improve coordination between U.S. law enforcement agencies and their foreign counterparts; and (3) promote robust compliance with international AML/CFT standards to reduce the risks posed by jurisdictional arbitrage. The following are recommendations in each of these areas.

A. Strengthen and Expand U.S. Law Enforcement Operational and Capacity-Building Efforts with Foreign Law Enforcement Partners

Expanding foreign partners' criminal justice sector capacity strengthens global law enforcement efforts and provides multiple benefits to the United States. It helps other nations address illicit activity where it originates and at its inception, to the benefit of victims, including U.S. citizens, around the world. It also improves the ability of foreign counterparts to aid the United States when our law enforcement agencies are investigating cross-border activities and request the assistance of those foreign partners in gathering evidence, seizing assets, and locating and disrupting criminal actors and infrastructure.

As noted, U.S.-provided capacity building for eligible countries is already taking place. The Department of State, using appropriations authorized under the Foreign Assistance Act, has funded the creation of the GLEN, as described above, and digital assets-related components are often also woven into the broader landscape of anticrime programming, whether delivered by U.S. government agencies or via multilateral partners. Continued support of the GLEN and these other programs is important and crucial to the United States' interest in ensuring that certain foreign partners are well positioned to aid in combating the threats posed by criminal misuse of digital assets and cybercrime.

While the GLEN's ongoing work for eligible countries is valuable and important, additional efforts to further international collaboration are needed, especially in areas where U.S. law enforcement has identified needs outside of the purview of current Foreign Assistance Act funding. First, U.S. law enforcement abilities would be significantly improved by expanding its overseas operational capacity (as opposed to training) to combat malicious criminal threats, particularly related to cybercrime and the illicit misuse of digital assets. As evidenced in law enforcement efforts targeting other types of criminal activity, increasing overseas operational capacity could permit more effective law enforcement information-sharing and could ensure the formation of the types of long-term collaborations between law enforcement personnel that can critically advance investigations and prosecutions.

Second, efforts to enhance the United States' ability to detect, investigate, prosecute, and otherwise disrupt the illicit use of digital assets would be more effective if funds for

international capacity building were allocated to international law enforcement partners, including those that the Department of Justice, as the lead domestic law enforcement agency, has identified based on specific operational needs.[22] The Department of Justice will initiate policy efforts towards developing and implementing a digital asset-specific capacity building initiative with the Department of State, the lead authority for providing and administering counter drugs and international law enforcement assistance, including capacity building under the Foreign Assistance Act. Such an initiative would ensure that the digital assets-related training and operational needs identified by U.S. law enforcement agencies are addressed in a manner that remains consistent with U.S. foreign policy and national security interests.

Third, it is crucial that any increase in foreign assistance-driven support be accompanied by an increase in the capacity of U.S. law enforcement implementers to deliver such assistance. In particular, the Department of Justice and law enforcement agencies should receive support to enhance their ongoing efforts to grow their capabilities to successfully disrupt criminal activity involving digital assets. Such support is critical not only to the success of U.S. law enforcement's own investigations and its integration into similar international efforts, but also to ensure that U.S. law enforcement has a cadre of subject matter experts available to provide up-to-date training and support to foreign counterparts on the evolving challenges posed by digital assets. Government-to-government training and technical assistance is the most effective way to achieve progress due to its ability to not only transfer needed skills but to strengthen international relationships with foreign counterparts, and to foster further cooperation and collaboration on cross-border investigations.

Finally, several additional avenues exist to support existing and additional capacity-building, training, and operational needs:

- Ensure that RLAs, ICHIPs, and other U.S. personnel have the flexibility to tailor training and/or investigative assistance to foreign nations for the particular types of digital asset-related crimes prevalent in the region;

- Include certain foreign law enforcement partners in domestic training programs, including at the National Computer Forensics Training Institute (NCFI), which is currently limited to providing its digital assets-related and other training to state, local, and tribal territories' personnel only; and

- Provide additional training that takes into account the cost and limited availability of proprietary blockchain analytics technology, and instructs foreign counterparts on the use of low-cost publicly available or open-source (free) tools in digital-asset investigations.

B. Deepen Information Sharing, Early Coordination, and Deconfliction Efforts

Although the United States has a proven history of working with its foreign law enforcement partners to meet the challenges posed by new criminal threats, the challenges posed by digital assets require continued and sustained attention and effort while the technology continues to evolve, and relevant laws and regulations are implemented and refined. In the meantime, international law enforcement efforts should be strengthened by developing more effective means of coordination across law enforcement partners, to identify emerging threats, threat actors, money

laundering techniques, and schemes to defraud victims worldwide, and to help deconflict efforts to hold criminals accountable.

To that end, this Report recommends the implementation of four actions for more effective transnational criminal investigations involving digital assets:

(1) Encourage information sharing, early coordination, and deconfliction of investigations across domestic and international law enforcement partners, to promote faster and more efficient coordination of criminal investigations involving digital assets, so that disruptive actions—such as infrastructure dismantlement, asset seizure, and/or arrests—can occur in a more timely and coordinated fashion;

(2) Support efforts to further international cooperation on the preservation and collection of records and evidence relating to crimes involving digital assets, including to facilitate expeditious and swift cross-border assistance for investigations, seizures, operations, and proceedings concerning digital asset-related crimes;

(3) Continue to provide policy support and subject matter expertise to international partners in the area of digital assets and associated emerging technologies; and

(4) Foster cooperation and partnerships with private sector entities operating in the digital asset space—both domestically and abroad—who seek to be responsible actors in the ecosystem, for purposes of strengthening collaborative efforts to root out illicit use of digital assets.

C. Address Jurisdictional Arbitrage Through Closing Gaps in AML/CFT Regulation and Supervision

Deficient AML/CFT regulatory and supervisory regimes in many jurisdictions present an opportunity for criminal actors to engage in jurisdictional arbitrage, purposely seeking to further their criminal activities in such jurisdictions. This presents a challenge to U.S. authorities' abilities to prevent or investigate a wide variety of illicit digital asset activity, as digital asset transactions related to crimes, such as ransomware and money laundering, frequently are cross-border by nature. According to the FATF, as of July 2021, most members of the FATF's Global Network had not yet implemented the revised FATF standards on virtual assets and VASPs in their national law. In fact, only 35 jurisdictions reported having an operational regime in line with the FATF standards for virtual assets and VASPs, and many of these are likely not effectively implemented in practice.[23] This environment creates gaps in AML/CFT controls in which foreign-located exchanges can allow criminal actors to access the international financial system without facing the scrutiny required by international standards and the regulators and supervisors of some national authorities.

The FATF has also noted progress in the development of technological solutions to enable the implementation of the "Travel Rule" for VASPs. The Travel Rule is a critical safeguard that helps VASPs identify, report, and disrupt illicit activity and can generate important information to help law enforcement and other competent

authorities investigate illicit financing. The FATF observed that the lack of implementation of Travel Rule requirements by jurisdictions was a disincentive to the private sector, particularly VASPs, to invest in the necessary technological solutions and compliance infrastructure to comply with the rule.[24] To minimize opportunities for criminal actors to exploit gaps in AML/CFT implementation across jurisdictions, the United States can:

(1) Continue to work through the FATF's Virtual Asset Contact Group to encourage and support countries in implementing the FATF recommendations, including the Travel Rule;

(2) Continue to engage bilaterally with countries to explain the FATF recommendations, understand challenges to implementation, and support countries in overcoming those challenges; and

(3) Encourage partners to examine and weigh the reputational and national security risks and policy implications associated with allowing certain virtual assets businesses to operate within their borders, especially those that brand themselves as "headquarters-less," eschew traditional notions of primary domicile and place of business, or resist application of laws or standards requiring transparency and compliance with AML/CFT and other legal requirements.

Some of these and related efforts will be explored in more detail in forthcoming reports written pursuant to Section 7(c) and Section 8(b) of the Executive Order.

CONCLUSION

Strengthening international law enforcement cooperation for detecting, investigating, prosecuting, and otherwise disrupting criminal activity related to digital assets is vital to the mitigation of illicit finance and national security risks posed by the misuse of such assets. Timely coordination and information sharing is essential to combat the growing use of digital assets to facilitate criminal activity, including money laundering, ransomware activities, cybercrime, fraud, theft, terrorist financing, and sanctions evasion. And given the global, cross-border nature of digital asset technologies, the U.S. government must continue its commitment to assisting our foreign partners in building their own operational capacity, as well as their regulatory and supervisory oversight of digital assets, for the mutual benefit of fostering capability to disrupt criminal activity involving these technologies across the globe. However, because the threat landscape for misuse of digital assets is constantly changing as the technology continues to grow and evolve in use and application, law enforcement must in turn continue its efforts to evolve to meet the challenge posed by criminal use of digital assets. Going forward, the Department of Justice and its law enforcement and regulatory partners will continue to explore new opportunities and ways to foster international coordination and collaboration to combat criminal activity related to digital assets.

ANNEX A
Illicit Use of Digital Assets

Criminals are increasingly leveraging features of digital assets to advance and conceal unlawful schemes. Digital assets can be an attractive method for quickly transferring value across international borders without any financial intermediary and sometimes with minimal transaction fees, especially in developing countries without a secure and widely available banking infrastructure. The global nature of blockchain technology also makes digital assets an attractive vehicle for malign actors to hide their financial transactions and transfer assets in a quick, efficient way outside of traditional regulatory oversight.

Digital assets are used to further a variety of different types of criminal activity, including the following types of crime.

Money Laundering

Digital assets and the exchanges trading them can offer opportunities for criminals to launder their illicit proceeds. A conservative estimate from one blockchain analysis firm reports that cybercriminals have laundered over $33 billion worth of cryptocurrency since 2017.[25] By conducting their transactions in cryptocurrency, criminals can avoid large cash transactions and mitigate the risk of suspicious transactions being frozen or reversed, financial transactions being traced, or banks notifying governments of suspicious activity. Non-existent or weak AML/CFT regulations in certain countries allow criminals to use false identities when creating online accounts to trade or exchange digital assets, if any identifying information is required to be submitted at all. Additionally, many criminals use a variety of obfuscation techniques to further divert investigators off their digital trail. Criminals can "chain-hop," that is, swap between various cryptocurrencies and affiliated blockchains, often in rapid succession. Launderers also utilize mixing and tumbling services, which pool together cryptocurrency transactions and then send the funds to designated recipients in a manner designed to conceal and obfuscate their source. Money mule networks are increasingly using cryptocurrency kiosks or cryptocurrency prepaid cards to launder funds both domestically and internationally.[26]

Ransomware

Cryptocurrency has been used for many years to facilitate cybercrime in a variety of ways, including to facilitate the purchase of online infrastructure and tools used to commit cybercrimes. More recently, it has helped fuel the rise of ransomware and other digital extortion activities. Ransomware is a form of malicious code that blocks access to a victim's computer system or data, often by encrypting data or files on computer networks to extort ransom payments from victims in exchange for a decryption key to restore a victim's access to their systems or data. In some cases, ransomware actors exfiltrate the victim's data before encrypting it, and send a ransom demand that includes a threat to release or publish the victim's data if the ransom is not paid. Ransomware actors often demand ransom payment in the form of digital currency. Many private sector companies have noted significant increases from year to year in the use of digital assets to collect ransomware payments and to launder the proceeds of fraud. [27]

Currently, the Department of Justice and law enforcement agencies are investigating over 100 different ransomware variants and ransomware groups that have caused billions of dollars in damage. The Department also has had some notable successes in disrupting ransomware activities over the last year, including the recovery of approximately $2.3 million in cryptocurrency paid as ransom by those responsible for the DarkSide ransomware incident targeting Colonial Pipeline.[28] The Department also announced charges against individuals suspected of deploying Sodinokibi/REvil ransomware against victim companies, including the arrest of the individual charged with the ransomware attack against Kaseya, a multinational information technology software company, as well as the seizure of $6.1 million in cryptocurrency paid in ransom to the group.[29]

Fraud and Theft

Some of the features of digital assets make them particularly attractive vehicles for multiple varieties of fraud and theft. Public reports and assessments by blockchain analysis companies estimate that, in total, more than $10 billion in cryptocurrency was stolen or scammed from victims in 2021, a substantial increase from the previous year.[30] One reason for the growth in stolen digital assets is the rise of so-called Decentralized Finance (DeFi) platforms.[31] DeFi refers to a class of digital asset protocols and platforms, some of which allow for automated peer-to-peer transactions without the need for an account or custodial relationship and often through the use of smart contracts. These protocols and platforms are open for anyone to use and provide an alternative to traditional financial intermediaries like banks or brokerages, as well as VASPs.[32]

Digital assets have been used in a variety of securities and commodities frauds, including theft of investor funds, Ponzi-like schemes, and frauds involving initial coin offerings (ICOs). In addition, digital assets have been stolen from victims of "romance" scams and confidence frauds, in which fraudsters, among other methods, assume online identities to befriend and persuade victims to purchase digital assets and ultimately transfer those assets to the fraudster or entities under their control.[33] In 2021 alone, the FBI's Internet Crime Complaint Center (IC3)—the website through which the public can report being victims of internet crimes to the FBI—received more than 4,300 complaints, detailing losses of more than $429 million from the victims of romance scams and confidence frauds. Victims also reported losses from fraudulent investment opportunities in digital assets, with losses in some cases into the hundreds of thousands of dollars per victim.[34]

Other scams involve "rug pulls," where, among other schemes, fraudsters develop new tokens and promote them to investors, who purchase the new tokens in the hopes the token's value will rise. However, the fraudulent developers eventually steal the investors' money and disappear, sinking the value of the new tokens to zero. Some commercial blockchain analysis companies estimate that DeFi users and investors suffered losses attributable to rug pulls totaling almost $3 billion last year alone.[35]

In addition to these fraud schemes, illicit actors, including cybercriminals and nation-state hackers, can steal cryptocurrency by exploiting security vulnerabilities in wallets and exchanges. Thieves can hack wallets and exchanges directly; engage in insider theft; or employ social engineering and other tools to obtain passwords and PINs from unsuspecting users. More sophisticated criminals may compromise the underlying code of these new platforms and steal the funds from DeFi projects,

leaving investors' accounts depleted. For instance, in March 2022, Lazarus Group, a DPRK state-sponsored cyber hacking group, stole over $600 million from a blockchain project linked to an online gaming platform.[36]

Narcotics Trafficking

Law enforcement has seen a significant increase in the use of cryptocurrency by transnational criminal organizations involved in the illicit drug trade. These organizations use cryptocurrency not only to facilitate drug transactions on darknet markets, but also to launder drug proceeds across international borders. As worldwide border restrictions and travel bans imposed during the COVID-19 pandemic complicated bulk cash smuggling operations, these organizations increasingly turned to cryptocurrency to move drug proceeds quickly, efficiently, and pseudonymously from the United States to other countries. Darknet marketplaces use software services such as Tor—a free and open-source software for enabling anonymous communication—that allow users to anonymously buy and sell illicit goods and services, including narcotics and other controlled substances. The most popular payment medium of exchange on these marketplaces is cryptocurrency, with increasing use of AECs. Tech-savvy drug cartels are increasingly using digital asset technology innovations to their advantage, requiring law enforcement to likewise increase their ability to follow the digital evidentiary trails.

Human Trafficking

Human traffickers have increasingly turned to cryptocurrency to promote illegal sex services and to launder their profits, although cryptocurrency is one of several payment options. Some trafficking groups use thinly veiled online advertisements to solicit customers by offering services in "adult entertainment" sections of classified advertisement publications. In cases where providers of online classified advertisements could no longer use major merchant processors like Visa and Mastercard for their advertisement fees, they turned to bitcoin for payments of these ads.[37]

Terrorism Financing

Terrorists and their supporters use digital asset platforms for crowdfunding campaigns to expand their base of support.[38] Violent extremist organizations even provide instructions on social media platforms on how to use cryptocurrency services to purchase and send digital assets to support their campaigns.[39] The global and distributed nature of digital asset platforms has also enabled terrorists to make peer-to-peer transfers to members of their organizations, circumventing the AML/CFT controls found in more traditional payment methods. As the use of digital assets expands, so too will terrorists' and their supporters' use of this technology. The growing popularity of virtual currency in countries where terrorism financing persists is of great concern.

Sanctions Evasion

In general, U.S. persons and other persons otherwise subject to the jurisdiction of OFAC, including firms that facilitate or engage in online commerce or process transactions using virtual currency, may not engage in transactions prohibited by OFAC sanctions regulations. These include

dealings with blocked persons or property or engaging in prohibited trade or investment-related transactions. Prohibited transactions include transactions that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate prohibitions imposed by OFAC under various sanctions authorities.[40] Violations of OFAC regulations may result in criminal or civil penalties.

Some of the evasive activities involving digital assets mirror those of traditional sanctions evasion activity: use of shell companies to conduct financial transactions; use of financial institutions in jurisdictions distinct from where the company is registered; and/or use of newly established accounts to receive funds from sanctioned entities. Yet, digital assets can uniquely help to facilitate some sanctions evasion activity, such as through the use of an exchange platform or foreign-located VASP in a high-risk jurisdiction with AML/CFT deficiencies, or the use of digital asset mixing or tumbling services to break the chain of custody on public blockchains or to further obfuscate transactions. Cryptocurrency's distributed and peer-to-peer format may allow sanctioned entities to bypass the financial controls built into the traditional financial marketplaces to enforce such sanctions. Additionally, nation-state hackers, such as those working for the DPRK, may steal cryptocurrency as a means to find alternative funding streams that reduce the impact of sanctions regimes.

Tax Evasion

The rise in the use of cryptocurrencies has provided additional avenues for tax evasion. Individuals and businesses are required by U.S. law to report income received in cryptocurrency on their tax returns. They may be tempted by the pseudonymous characteristics of cryptocurrencies, however, to omit income received in cryptocurrencies on their tax returns. This unreported income may consist of, among other things, unreported capital gains, wages, and other forms of compensation (including from mining digital assets); gross business receipts; and gambling winnings. Businesses may also try to fraudulently reduce their reported income by using cryptocurrencies as part of false invoicing schemes. Criminals are also increasingly using cryptocurrencies to hide the profits of their criminal schemes from tax authorities.

ANNEX B
Examples of Successful Cross-Border Collaboration on Digital Asset Investigations

Strong cooperation and coordination among the Department of Justice, its law enforcement and regulatory partners, and their international counterparts have been crucial to combatting the illicit use of digital assets. Successful enforcement and regulatory actions have included takedowns of illicit exchanges, money laundering platforms, and darknet markets; the apprehension of hackers, money launderers, and fraudsters who have targeted victims from across the globe; and the seizure and recovery of digital assets and other proceeds of criminal activity.

1. Exchanges and Money Laundering Platforms, Including Mixers and Tumblers

Crimes involving digital assets are often facilitated through the illicit use of exchanges and money laundering platforms, including mixers and tumblers. Criminal actors conducting a wide variety of crimes use these platforms to further their activities, including by cashing out the proceeds of their crimes and taking measures to obfuscate their financial trail and identities. Recognizing the importance of investigating and disrupting such platforms in enforcing against the misuse of digital assets, the Department of Justice has been working to disrupt such platforms since before the advent of cryptocurrency, such as in the prosecution of e-Gold in 2007. As the use of digital assets has grown, the Department of Justice's efforts have also expanded to include criminal activity involving other money laundering platforms.

The following examples of successful investigations involving exchanges and platforms illustrate instances in which law enforcement, with strong international cooperation from foreign law enforcement partners, has been able to overcome the challenges posed by the global nature of digital assets investigations.

Liberty Reserve

On May 28, 2013, the Department of Justice announced charges against Liberty Reserve, at the time one of the world's largest digital currency companies, and seven of its principals and employees for running a multi-billion-dollar money laundering scheme. Liberty Reserve had more than one million users worldwide, including more than 200,000 users in the United States, who conducted approximately 55 million transactions—virtually all of which were illegal—and laundered more than $6 billion in suspected proceeds of crimes including credit card fraud, identity theft, investment fraud, computer hacking, child pornography, and narcotics trafficking.

The investigation by IRS-CI's Global Illicit Finance Team, the USSS, HSI, and others, revealed that the defendants protected the criminal infrastructure of the company by, among other things, lying to AML authorities in Costa Rica and pretending to shut down Liberty Reserve after learning the company was being investigated. They then continued operating the business through a set of shell companies, moving tens of millions of dollars through shell company accounts maintained in Cyprus, Russia, China, Hong Kong, Morocco, Spain, Australia, and elsewhere.

When U.S. authorities shut down Liberty Reserve in 2013, it was believed to be the largest international money laundering prosecution in history, involving law enforcement actions in 16 countries, including Costa Rica, the Netherlands, Spain, Morocco, Sweden, Switzerland, Cyprus, Australia, China, Norway, Latvia, Luxembourg, the United Kingdom, Russia, Canada, and the United States. In particular, U.S. law enforcement collaborated with the Judicial Investigation Organization in Costa Rica; the National High Tech Crime Unit in the Netherlands; the Spanish National Police, Financial and Economic Crime Unit; the Cyber Crime Unit at the Swedish National Bureau of Investigation; and the Swiss Federal Prosecutor's Office. A collective international effort to follow the flow of digital assets in the United States and around the world was key to the operation's success.

BTC-e

In 2017, the Department of Justice announced the indictment of the virtual currency exchange BTC-e and one of the exchange's principal operators. The investigation, led by the USSS, IRS-CI, and the FBI, established that BTC-e received more than $4 billion worth of bitcoin over the course of its operation. The indictment alleged that BTC-e facilitated transactions for cybercriminals worldwide and received criminal proceeds from numerous computer intrusions—including the hack of Mt. Gox, an earlier virtual currency exchange that eventually failed, in part due to losses attributable to the hacking—ransomware scams, identity theft schemes, corrupt public officials, and narcotics distribution rings. In conjunction with the Department of Justice's criminal charges, FinCEN assessed a $110 million civil penalty against the exchange for willfully violating he Bank Secrecy Act (BSA), and a $12 million penalty against the exchange's operator.[41]

BTC-e is only one example in a series of cases in which the Department of Justice has pursued criminal charges against cryptocurrency exchanges for operating as unlicensed money transmitting business.[42] It is also an example of the Department's resolve to prosecute foreign-located entities and individuals in the cryptocurrency context. BTC-e operated globally as an unlicensed virtual currency exchange to launder and liquidate criminal proceeds from virtual currency to fiat currency. In doing so, it relied on the use of shell companies and affiliated entities that were similarly unregistered with FinCEN. According to its now-defunct website, BTC-e purported to be based in Eastern Europe. BTC-e's managing shell company, Canton Business Corporation, was registered in the Seychelles, and its web domains were registered to shell companies in, among other places, Singapore, the British Virgin Islands, France, and New Zealand.

Helix

On February 13, 2020, the Department of Justice announced the indictment and arrest of the administrator of Helix, a darknet cryptocurrency laundering service. This case was investigated by IRS-CI and the FBI, with assistance from the Department of State's Diplomatic Security Service. According to the indictment, Helix functioned as a bitcoin mixer or tumbler. The indictment charged Helix with laundering over $300 million of bitcoin, which represented the proceeds of illicit narcotics sales and other criminal transactions. 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.[43] Separately, FinCEN issued a $60 million civil money penalty against Helix on October 19, 2020.[44] On August 18, 2021, the administrator pleaded guilty to money laundering conspiracy arising out of his operation of Helix.[45]

2. Darknet Markets

Many cryptocurrency-related crimes are made possible through the operation of online black markets on the dark web. Indeed, much of the illicit conduct involving digital assets occurs via darknet websites and marketplaces that allow criminals around the world to connect in unregulated virtual bazaars with a great deal of anonymity. Darknet markets are online marketplaces that offer illicit goods and services for sale, often using cryptocurrencies as a method of payment. Drugs, stolen information, weapons, and illicit services, such as hacking-for-hire, are common items for sale in these markets. The transactions in darknet markets are anonymized using the Tor network, which creates security and anonymity for both buyers and vendors on the sites. Transactions take place via cryptocurrencies, like bitcoin, and sometimes involve additional anonymity-enhancing measures to protect the seller and buyer. The payment is typically held in escrow by the site administrators until the sale is completed.

These illicit marketplaces offer the opportunity not only to buy and sell illegal goods and tools for committing crimes, but also to launder money and hide ill-gotten gains. As a result, darknet markets are a natural place for digital assets to be widely used and exploited. Working closely with its international law enforcement partners, the Department of Justice's efforts to dismantle these virtual black markets continue in earnest. Some examples are described below.

Silk Road

The Department of Justice's prosecution of darknet markets began with Silk Road, a massive and anonymous marketplace that operated using the Tor network. From its inception in 2011 until October 2013, when it was seized by law enforcement, the Silk Road website was the most sophisticated and extensive criminal marketplace on the Internet. During its two-and-a-half years in operation, Silk Road was used by thousands of drug dealers and other unlawful vendors located around the world, including in the United States, Germany, the Netherlands, Canada, the United Kingdom, Spain, Ireland, Italy, Austria, and France, to distribute hundreds of kilograms of illegal drugs and other illicit goods and services.[46]

On October 1, 2013, Ross Ulbricht—Silk Road's creator and administrator—was arrested and charged by criminal complaint with narcotics trafficking conspiracy, computer hacking conspiracy, and money laundering conspiracy. The investigation and takedown were the culmination of a multi-agency collaboration with foreign law enforcement, including the Australian Federal Police, the Irish Republic's Computer Crime Investigation Unit of the An Garda Siochana, the Reykjavik Metropolitan Police of the Republic of Iceland, and the French Republic's Central Office for the Fight Against Crime Linked to Information Technology and Communication.

Operation Bayonet (AlphaBay and Hansa)

Operation Bayonet and its coordinated takedowns of AlphaBay Market and Hansa Market, arrests of these sites' administrators, and seizure of their criminally derived assets, is another example of close and successful collaboration between the Department of Justice, FBI, DEA, IRS-CI, HSI, and an array of foreign partners to disrupt harmful and global crimes involving cryptocurrency. At the time of its seizure in July 2017, AlphaBay was the world's largest darknet marketplace, whose over-200,000 accountholders used it to conduct over $750 million worth of transactions involving illegal drugs, firearms, malware, and toxic chemicals.[47] Operation Bayonet was led by the Department of Justice, FBI, DEA, and the Netherlands's Dutch National Police, and involved cooperation from law enforcement partners in Thailand, Lithuania, Germany, Canada, the United Kingdom, and France, as well as Europol.[48] Evidence of the crimes committed on AlphaBay and Hansa have supported many criminal investigations and prosecutions throughout the world.

Dream Market

In October 2018, as a result of a prosecution brought by the Department of Justice, a French national serving as an administrator and moderator of the darknet marketplace Dream Market was sentenced to 20 years in federal prison for narcotics trafficking and money laundering.[49] Following the dismantling of Silk Road and AlphaBay, Dream Market had become one of the largest darknet criminal marketplaces, and all of its items and services were offered for sale in exchange for bitcoin or other peer-to-peer cryptocurrencies. The prosecution was a result of collaboration between DEA, FBI, IRS-CI, and various foreign law enforcement partners, including Europol, Finnish National Police, Finnish International Judicial Administration of the Ministry of Justice, Dutch National Police, and the French Ministry of Justice and Direction Interregionale de la Police Judiciaire.

Wall Street Market

In May 2019, following a two-year international investigation involving multiple U.S. law enforcement agencies and authorities in Germany and the Netherlands, the Department of Justice charged three German nationals with being the administrators of Wall Street Market (WSM). WSM, at the time one of the world's largest dark web marketplaces, allowed vendors to sell a wide variety of contraband, including illegal narcotics, counterfeit goods, and malicious computer hacking software.[50] For nearly three years, the defendants operated WSM on the dark web. In April 2019, the three defendants conducted an "exit scam," taking all the virtual currency held in marketplace escrow and user accounts—believed by investigators to be approximately $11 million—and diverting the money to their own accounts.[51] A fourth individual, a resident of Sao Paulo, Brazil, was also charged in connection with the offense. The DEA, FBI, IRS-CI, and the United States Postal Inspection Service led this investigation in collaboration with the German Federal Criminal Police, the German Public Prosecutor's Office in Frankfurt, the Dutch National Police, the Netherlands National Prosecutor's Office, the Federal Police of Brazil, Europol, and Eurojust.

DeepDotWeb

A coordinated international investigation led to the takedown of DeepDotWeb (DDW), a website operating as a key gateway to darknet marketplaces that provided users with direct access to numerous online darknet markets. In exchange, the administrators received kickback payments in cryptocurrency, representing commissions on the proceeds from each purchase of illegal goods made as a result of a referral from the DDW website. On May 6, 2019, the FBI and its international partners in France and Israel arrested the top administrators of DDW. One of the administrators was arrested at the airport in France while traveling from Israel to Brazil. Several searches, arrests, and interviews of co-conspirators took place simultaneously in Germany, the Netherlands, Israel, the United Kingdom, and Brazil. These actions also lead to the court-ordered seizure of the DDW website and technical infrastructure in Germany, Israel, and the Netherlands. In total, the operation included the cooperation of nine law enforcement agencies spanning seven countries, all acting in unison on the same day.

Welcome to Video

In October 2019, the Department of Justice announced the indictment of the alleged operator of Welcome to Video, the world's largest online child sexual exploitation darknet market at the time of its seizure. Welcome to Video was funded by bitcoin. Through the sophisticated tracing of bitcoin transactions, law enforcement was able to determine the location of the darknet server, identify the administrator of the website, and ultimately track down the website server's physical location in South Korea. The administrator of Welcome to Video was arrested and convicted of charges brought in South Korea. In addition to the administrator, law enforcement arrested and charged at least 337 users of the site across the United States and around the world. The globally coordinated law enforcement operation targeting Welcome to Video and its users led to the rescue of at least 23 minor victims who were actively being abused, allegedly by the site's users.[52] The international investigations were led by the IRS-CI, HSI, and the United Kingdom's National Crime Agency (NCA), with coordination with and assistance from the Korean National Police of the Republic of Korea and the German Federal Criminal Police.

Operation DisrupTor

In 2020, the Joint Criminal Opioid and Darknet Enforcement (JCODE) team partnered with Europol in Operation DisrupTor, a coordinated effort to disrupt opioid trafficking on the darknet. The operation involved law enforcement partners in approximately 10 countries and demonstrated the partnership between JCODE and Europol against the illegal sale of drugs and other illicit goods and services. Operation DisrupTor resulted in more over 170 arrests worldwide, and the seizure of weapons, drugs, and over $6.5 million in illicit proceeds, including cryptocurrency.[53]

Hydra Market

On April 5, 2022, the Department of Justice announced the seizure of Hydra Market (Hydra)—at the time, the world's largest and longest running darknet market—in collaboration with the German

Federal Criminal Police.[54] In 2021, Hydra accounted for an estimated 80% of all darknet market-related cryptocurrency transactions, and between 2015 and its seizure, the marketplace received approximately $5.2 billion in cryptocurrency. In addition to the seizure of the Hydra servers, German law enforcement seized cryptocurrency wallets containing approximately $25 million worth of bitcoin. In conjunction with the shutdown of Hydra, the Department of Justice also announced criminal charges against a Russian national for conspiracy to distribute narcotics and conspiracy to commit money laundering in connection with his operation and administration of the servers used to run Hydra. This investigation was led by DEA's Miami Field Division, FBI, IRS-CI, U.S. Postal Inspection Service, and HSI with the support and coordination by the Department of Justice's multi-agency Special Operations Division and the JCODE Team.

In conjunction with the shutdown of Hydra, Treasury sanctioned the darknet market and over 100 virtual currency addresses associated with Hydra's operation that had been used to conduct illicit transactions. This represents the first sanctions action by Treasury against a darknet market.

3. Cybercrime

Cryptocurrency has also been used in a variety of cybercrimes, including to help fuel the recent growth of ransomware and other digital extortion against businesses and entities. The following recent examples highlight how international cooperation has helped disrupt cryptocurrency-related cybercrime.

Twitter Hack

On July 14, 2020, malicious actors targeted Twitter and compromised numerous high-profile accounts, including those used by high-level government officials. For several hours, the malicious actors used the compromised accounts to tweet out a scam message that instructed people to send bitcoin to an address in return for double their money. The incident occurred at the height of the COVID-19 pandemic, when many high-profile political and business leaders were using Twitter as a platform to communicate with the public.

In response, on July 16, 2020, FinCEN issued an alert warning financial institutions of the scam and directing them to identify and report suspicious transactions potentially associated with the hack as quickly as possible.[55] On July 31, 2020, U.S. law enforcement agents, led by IRS-CI, along with international partners, conducted a coordinated takedown to arrest two subjects, including the primary perpetrator of the activity, and executed search warrants in the United States and the United Kingdom. As a result of the group's efforts, the main subject was quickly apprehended, eventually pleaded guilty, and received a three-year prison sentence. The case team identified additional co-conspirators through the investigation, as well as further victims, and through law enforcement actions mitigated a much larger threat. International partners also successfully searched a subject in England and searched and arrested another subject in Spain.[56] U.S. law enforcement coordinated with the Netherlands, Spain, and the United Kingdom. Efforts by IRS-CI, FBI, USSS and state and local law enforcement partners resulted in successful disruptive actions, including searches, seizures, interviews, and proffers, that ultimately led to the dismantlement of the group responsible for the July 2020 Twitter hack.

Sodinokibi/REvil Ransomware

The Department of Justice collaborated closely with its international partners[57] in a November 2021 action against two foreign nationals charged with deploying Sodinokibi/REvil ransomware to harm businesses and government entities in the United States. Using Sodinokibi/REvil ransomware, one defendant allegedly left electronic notes in the form of a text file on the victims' computers. The notes included a Tor address, as well as a link to a publicly accessible website address that the victims could visit to recover their files. Upon visiting either website, victims were given a ransom demand and provided a cryptocurrency address to use to pay the ransom. One of the alleged perpetrators was arrested and extradited with the help of authorities in the Republic of Poland, and multiple locations were searched with the assistance of the National Police of Ukraine and the Prosecutor General's Office of Ukraine. In addition, law enforcement seized $6.1 million in funds traceable to alleged ransom payments received by a Sodinokibi/REvil actor.

NetWalker Ransomware

In January 2021, the Department of Justice announced a coordinated international law enforcement action, led by the FBI, with substantial assistance from the Bulgarian authorities, to disrupt NetWalker ransomware, which affected companies, municipalities, hospitals, law enforcement, emergency services, school districts, colleges, and universities, among others. Malicious cyber activities specifically targeted the healthcare sector during the COVID-19 pandemic, taking advantage of the global crisis to extort victims. The action included charges against a Canadian national in relation to ransomware incidents in which tens of millions of dollars were allegedly obtained, the seizure of approximately $454,530.19 in cryptocurrency from ransom payments, and the disablement of a dark web hidden resource used to communicate with ransomware victims.

4. Fraud and Theft

As the growth of the digital assets market continues, frauds and thefts perpetuated through digital assets have also been on the rise, and the cross-border reach of these schemes, with targets and victims located throughout the world, necessitates cooperation with international partners. BitConnect is one example of the necessity of international cooperation and information sharing to address the global nature of digital asset fraud and theft.

BitConnect

On September 1, 2021, the Department of Justice announced the guilty plea of a participant in a massive conspiracy involving BitConnect, a cryptocurrency investment scheme that defrauded investors from the United States and abroad of over $2 billion.[58] The Department of Justice's and FBI's complex investigation into the BitConnect conspiracy involved multiple law enforcement partners, including the IRS Financial Investigations and Border Crimes Task Force, as well as active collaboration with the SEC and the Australian Securities and Investments Commission. The global span of the victim base required international cooperation and information sharing with more than a dozen countries—to include Australia, Finland, Indonesia, Israel, India, Malaysia, Thailand, United Arab Emirates (UAE), United Kingdom, Ukraine, and Vietnam—both for evidence collection and victim restitution.[59]

Other International Collaboration Efforts

Department of Treasury

Office of Terrorism and Financial Intelligence (TFI)

Treasury has worked with international counterparts on several occasions to take action targeting illicit activities in the digital assets area and to foster stronger AML/CFT programs abroad to better protect against exploitation by illegal actors.

In September 2021, for the first time, Treasury's OFAC designated a virtual currency exchange—SUEX—for its part "in facilitating transactions for ransomware actors."[60] In addition, OFAC published an "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,"[61] which provided guidance to the virtual currency industry.

In November 2021, OFAC designated virtual currency exchange Chatex "for facilitating financial transactions for ransomware actors."[62] Treasury's investigation "benefitted immensely from close coordination . . . with partners across Latvian and Estonian government agencies, including their information sharing and swift action."[63] Specifically, Latvian government authorities immediately suspended the operations of Chatextech, an affiliate of Chatex; assessed a fine for breaches of company registration and business conduct laws and regulations; and planned to identify current and former Chatextech board members, all non-Latvian nationals, in Latvia's registry of high-risk individuals. In addition, the Estonian Financial Intelligence Unit revoked the license of related entity Izibits OU following consultation with Treasury.

In April 2022, OFAC designated virtual currency exchange Garantex.[64] This action followed close coordination with Estonian authorities, which had revoked Garantex's license to provide virtual currency services in February 2022. Garantex lost its license after Estonia's Financial Intelligence Unit revealed critical AML/CFT deficiencies and found connections between Garantex and wallets used for criminal activity.

More broadly, Treasury regularly engages bilaterally and through multilateral forums, like the FATF, to encourage and support countries with implementing the FATF standards for virtual assets and VASPs and discuss illicit financing risks associated with virtual assets.

Internal Revenue Service-Criminal Investigation (IRS-CI)

IRS-CI is leading Treasury's international collaboration efforts regarding criminal tax enforcement and money laundering. In 2018, leaders of tax enforcement authorities from Australia, Canada, the Netherlands, the United Kingdom, and the United States established the joint operation alliance, known as the J5, to increase collaboration in the fight against international and transnational tax crime and money laundering. J5 members meet annually to exchange information and identify offshore tax evaders and international organized crime groups using digital asset technology to commit crimes. In these annual meetings, investigators, cryptocurrency experts and data scientists

work together in a coordinated effort to track down and identify individuals perpetrating tax crimes around the world. Real-world data sets from each country are shared to make connections that current individual efforts would take years to make without this collaborative effort. These collaborations have resulted in significant prosecutions. J5 partners also assisted with the prosecution of Canada-based firm Sky Global. Sky Global was charged with intentionally participating in a criminal enterprise that facilitated the transnational distribution of narcotics through the sale and service of encrypted communications devices.

Securities and Exchange Commission

The SEC has brought numerous enforcement actions relating to digital assets.[65] A number of those actions have benefited from cooperation with foreign authorities. Assistance provided by foreign authorities typically includes information gathering, such as obtaining documents and investigative testimony from overseas witnesses, and tracing, freezing and repatriating funds located abroad.

For example, in *SEC v. PlexCorps*, No. 17-cv-07007 (E.D.N.Y.), the SEC cooperated extensively with Quebec's Autorité des marchés financiers (QAMF) to freeze the assets of and eventually obtain favorable judgments against the Quebec-based promoters of a multi-million-dollar initial coin offering, which the SEC alleged was an unregistered and fraudulent offer and sale of securities. The cooperation involved, among other things, the exchange of information pursuant to the SEC's MMoU with the QAMF, the taking of testimony in Quebec under The Hague Convention, and the eventual combination of recovered investor funds for a single distribution of monies to PlexCorps victims, with approval by both U.S. and Quebec tribunals and regulatory authorities. Additional cooperation and assistance were provided by Ontario Securities Commission, the Hong Kong Securities and Futures Commission, the French Autorité des marchés financiers, the Financial Services Agency of Japan, the United Kingdom Financial Conduct Authority, the British Columbia Securities Commission, the Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), the Gibraltar Financial Services Commission, and the Monetary Authority of Singapore.[66]

In *SEC v. Telegram Group, Inc., et al.*, No. 19-cv-09439 (S.D.N.Y.), the SEC sought and obtained the cooperation of nearly a dozen foreign authorities to obtain information. In that action, the SEC alleged that Telegram engaged in an unregistered offer and sale of securities. The litigation resulted in Telegram returning more than $1.2 billion to harmed investors, paying $18.5 million in civil penalties, and being enjoined from distributing its crypto-asset—the Gram token.[67]

Commodity Futures Trading Commission

The CFTC is an independent agency that regulates the U.S. derivatives markets, which includes futures, swaps, and options on commodities and futures. As part of that mandate, the CFTC regulates derivatives markets where the underlying commodity is a digital asset, including Bitcoin or Ether.[68] The CFTC's enforcement program also has broad anti-fraud and anti-manipulation authority over commodities in interstate commerce, including digital assets such as Bitcoin and Ether.

Since 2015, the CFTC has brought over 50 enforcement actions involving digital assets, and regularly cooperates with foreign counterparts in connection with enforcement investigations, including those relating to digital assets. These actions include 23 matters filed in fiscal year 2021 and involve defendant entities located in the United States and abroad.[69] For example, in *In re Tether* (CFTC Dkt. No. 22-04), the CFTC collaborated with numerous international partners in bringing an action against the four offshore entities behind the Tether U.S. dollar stablecoin (USDT) for making untrue or misleading statements regarding fiat currency reserves purportedly backing USDT tokens in circulation.[70]

In *CFTC v. HDR Global Trading,* No. 20-cv-8132 (S.D.N.Y.), the CFTC obtained favorable judgments against the operators of the BitMEX trading platform for facilitating cryptocurrency derivatives transactions and leveraged retail commodity transactions in the United States, and for accepting funds from U.S. persons, without being registered as required; for failing to implement a Customer Information Program and KYC procedures that would enable to identification of U.S. persons using the platform; and for failing to implement an adequate AML program. In connection with the resolution of that action and a parallel filing by FinCEN, BitMEX paid a $100M in civil penalties, undertook remedial measures to develop AML and user verification programs, and ceased operating in the United States. Assistance was provided by the Hong Kong Securities and Futures Commission, the Bermuda Monetary Authority, and the Financial Service Authority Seychelles.[71] Further, in *CFTC v. McAfee,* No. 21-cv-1919 (S.D.N.Y.), the CFTC, along with the Department of Justice and the SEC, took action against the operators of an international digit asset "pump and dump" scheme who secretly accumulated positions in various digital assets, deceptively promoted the assets on social media while concealing their holdings, and then, once prices rose, secretly sold off their holdings.[72]

ANNEX C
International Training and Outreach Efforts

Building the law enforcement and prosecutorial capacity of other countries provides multiple benefits. It allows other nations to address illicit financial activity, terrorism, and other transnational crime at the source, for the benefit of citizens around the world. It also improves the ability of foreign counterparts to aid the United States when our law enforcement agencies are investigating cross-border activities and request the assistance of those foreign partners in tracking fugitives, gathering evidence, or seizing assets. Examples of the many training and outreach programs our domestic agencies and regulators are providing to our foreign law enforcement partners are discussed below.

Department of State

The U.S. Transnational and High-Tech Crime Global Law Enforcement Network (GLEN) is a U.S. Department of State Bureau of International Narcotics and Law Enforcement Affairs (DOS/INL)-funded program and consists of a partnership between DOS/INL, FBI, CCIPS and the Office of Overseas Prosecutorial Development, Assistance and Training (OPDAT). GLEN is a worldwide law enforcement capacity building network of ICHIP Attorney Advisors, computer forensic analysts, and federal law enforcement agents who deliver training and technical assistance to foreign law enforcement, prosecutorial, and judicial partners to combat intellectual property and cybercrime activity, as well as to provide training in the collection and use of electronic evidence.

The GLEN's objective is to promote the rule of law and to protect Americans from criminal threats emanating abroad by delivering targeted training to encourage immediate improvements as well as long-term institutional change to combat computer and intellectual property crimes. This assistance includes training workshops, legislative review, case-based mentoring, skills-development, and promoting institutional reform such as the formation of specialized units to address these criminal threats.

Currently, ICHIP attorneys are posted to regional positions in Africa (Abuja, Nigeria and Addis Ababa, Ethiopia); Asia (Hong Kong, S.A.R.; Bangkok, Thailand; and Kuala Lumpur, Malaysia); Europe (Bucharest, Romania; Zagreb, Croatia; and The Hague, Netherlands); and the Western Hemisphere (Panama City, Panama and Sao Paulo, Brazil). Two subject-matter expert ICHIPs—the Global ICHIP for Internet-based Fraud and Public Health and the Global ICHIP for Dark Web and Cryptocurrency—as well as the Department of Justice's computer forensic analysts and law enforcement officials with intellectual property and cybercrime expertise, also form part of the GLEN.

The Department of State also provides voluntary funding to multilateral partners like the UN Office on Drugs and Crime, the Organization of American States, INTERPOL, and the Council of Europe, to deliver cybercrime training and technical assistance programs which also often address criminal misuse of digital assets.

Department of Justice

The Department of Justice has developed key partnerships to detect, prosecute, and otherwise disrupt criminal activity facilitated by the illicit use of digital assets.

OPDAT administers technical and developmental assistance to enable foreign institutions and law enforcement personnel to combat particular categories of crime, which in recent years have included those involving the use of digital assets. Part of OPDAT's program includes the deployment of RLAs to approximately 60 countries as of FY 2022. These RLAs support a variety of criminal justice projects to include: (1) capacity building for investigators, prosecutors, and judges in the form of case-based mentoring and workshops; (2) enhancing bilateral and international cooperation between prosecutors and law enforcement on terrorism and AML matters; (3) addressing substantive gaps in criminal legislation, regulations, and court rules, including in the areas of digital asset criminal investigations, and investigative techniques; and (4) responding to key legislative and capacity development opportunities in the area of terrorism, money laundering, asset forfeiture, terrorism financing, and cybercrime. The National Security Division's Counterterrorism Section (CTS) works closely with OPDAT to support OPDAT's projects and programming, including by providing training on the prosecution of terrorism financing using digital assets. CTS attorneys have provided such training virtually for new and onboarding RLAs and in person for State and Treasury Department personnel, most recently in April 2022.

CCIPS attorneys and its Cybercrime Lab collaborate extensively with foreign and domestic law enforcement partners on criminal investigations and prosecutions involving digital assets and cryptocurrency. These matters involve malware and ransomware activities and associated identity and financial thefts; the use of money laundering networks, mixers and tumblers, and cryptocurrency exchanges to launder the proceeds of cybercrime and cyber-enabled crime; and the operation and use of darknet markets to buy and sell contraband using cryptocurrency, among others. CCIPS also provides training and technical assistance to domestic and foreign law enforcement and prosecutors on the technologies underlying digital assets and the crimes they are used in; infrastructure and asset seizures; and the global coordination of these complex investigations and related operations.

In 2018, MLARS developed a Digital Currency Initiative (DCI) specializing in cryptocurrency-related prosecutions, including the recovery of cryptocurrency assets. The DCI provides both international and domestic legal guidance and support to investigators, prosecutors, and government agencies on cryptocurrency prosecutions, seizures, and forfeitures. The DCI provides cryptocurrency-related training and engages in policy dialogue concerning legislation, forfeiture, and prosecution. Building on this Initiative, in October 2020, the Department of Justice issued the Attorney General's Cryptocurrency Enforcement Framework articulating the concerns and challenges associated with this emerging technology.

Most recently, in furtherance of the goal of developing strong international and interagency partnerships, Deputy Attorney General Lisa O. Monaco announced the formation of NCET in November 2021 to investigate and support complex investigations and prosecutions of criminal misuses of cryptocurrency. Comprised of more than a dozen federal prosecutors and support staff,

including experts detailed from CCIPS, MLARS, and several U.S. Attorneys' offices, the NCET has a particular focus on crimes committed by exchanges, mixing and tumbling services, and money laundering infrastructure actors. It also assists in tracing and recovery of assets lost to fraud and extortion, including cryptocurrency payments to ransomware groups. The NCET builds upon and strengthens the Department of Justice's capacity to dismantle entities that enable criminal actors to flourish and profit from abusing cryptocurrency platforms.

Recognizing the global nature of the challenge posed by the illicit use of digital assets, international partnerships and capacity building are key parts of the NCET's mission. NCET members have conducted or will be conducting a variety of international trainings concerning digital asset prosecutions, including to the Criminal and Legal Affairs Subgroup of the G7's Roma/Lyon Group, the U.S.-European Cryptocurrency Working Group, the Counsel of Europe's European Conference of Prosecutors, and Europol's Virtual Currency Conference at The Hague, Netherlands.

Federal Bureau of Investigation

The FBI is an intelligence-driven and threat-focused national security organization with both intelligence and law enforcement responsibilities. With its cyber and investigative expertise, the FBI has been at the center of efforts to detect, investigate, and prosecute criminal activity related to digital assets worldwide, including through its 63 Legal Attaché (Legat) offices and 30 sub-offices in key cities around the globe, providing coverage for more than 180 countries, territories, and islands. To further those efforts, in February 2022, the FBI formed the 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,[73] the VAU will centralize 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 will help 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 used this curriculum to train thousands of FBI employees and partners around the globe.

The FBI's Hi-Tech Organized Crime Unit (HTOCU) manages the Joint Criminal Opioid and Darknet Enforcement (JCODE) team, which was established in January 2018. JCODE was created to lead and coordinate government efforts to detect, disrupt, and dismantle major criminal enterprises reliant upon the darknet for trafficking opioids and other illicit narcotics, along with identifying and dismantling their supply chains. JCODE shares resources and expertise across multi-agency partners and leverages the investigative power of federal and international partnerships to combat the borderless nature of online criminal activity. The JCODE team currently consists of 11 entities that provide personnel to support the mission and partners with Europol in major operations conducted annually. It relies heavily on international relationships for proper deconfliction and coordination to better target this global threat.

International Trainings and outreach presentations from 2016 through the end of June 2022 include virtual and in-person trainings to law enforcement partners from 66 countries. Further, the FBI has distributed resources for guidance on identifying digital assets and seizure best practices, to over 91 countries.

Year	2016	2017	2018	2019	2020	2021	2022
Estimated Reach (# of participants)	157	493	286	532	85	884	646
Trainings/Outreach	5	21	8	6	1	34	21

Finally, the FBI and the National Cyber Investigative Joint Task Force (NCIJTF) host an annual Virtual Currency Symposium. Starting in 2016, excluding 2020 and 2021 due to COVID restrictions, this three-day event brings subject matter experts from U.S. federal, state, and local law enforcement agencies, regulatory agencies, intelligence community agencies, Department of Defense agencies, prosecutorial agencies, international law enforcement partners, as well as industry and academia partners together to discuss all matters concerning digital assets and how the groups can collaborate together and share information.

Drug Enforcement Administration (DEA)

The DEA is a key player in narcotics investigations involving the use of cryptocurrency on darknet markets and by transnational criminal organizations (TCO).[74] The DEA works closely with foreign partners on drug enforcement, including matters related to cryptocurrency, through its 92 foreign offices located in 69 countries, as well as its Special Operations Division (SOD) at DEA Headquarters and its domestic offices throughout the United States.

DEA is prioritizing the development of deep technical expertise, robust capabilities, and strong international partnerships to combat the use of cryptocurrency to facilitate drug trafficking within the United States and transnationally. DEA is investing in specialized training for new and seasoned agents, investigators, and analysts, as well as cutting-edge tools necessary to trace complex cryptocurrency transactions. SOD serves as a critical coordination and deconfliction center for drug trafficking cases, including those matters involving cryptocurrency. Through SOD, DEA will continue to ensure cooperation among domestic and foreign law enforcement in transnational cases and will also enhance those investigations through advanced analytic techniques.

Since 2015, DEA has provided cyber investigation and cryptocurrency training to international counterparts from around the world, including to law enforcement partners in Canada, the Netherlands, Singapore, Thailand, Peru, El Salvador, Finland, South Africa, Romania, France, England, and Australia. In April 2018, for example, DEA conducted a two-day working group meeting in South Africa on the dark web and cryptocurrency as it relates to drug trafficking. Fifty members of the South African Police Service and South Africa's Financial Intelligence Centre attended the working group.

DEA's International Training Unit also created a cyber exploitation and investigation course for International Law Enforcement Academies (ILEA) in Africa, Europe, and Central America. DEA's International Training Unit and Cyber Training Unit conducted two courses in 2021 and two courses in 2022 in El Salvador on cryptocurrency tracing and how it is used in darknet market investigations. Members of law enforcement from Argentina, the Bahamas, Belize, Brazil, Chile, Costa Rica, Ecuador, El Salvador, Guatemala, Mexico, Panama, Paraguay, and Uruguay, among other countries, attended the ILEA trainings.

Department of Treasury

Office of Terrorism and Financial Intelligence (TFI)

FinCEN serves as the financial intelligence unit (FIU) for the United States and has primary responsibility for administering and enforcing the BSA, which requires persons or entities that provide certain services related to digital assets to register with Treasury and implement AML/CFT measures.

Given the cross-border nature of digital asset transactions, there is a clear need for Treasury and FinCEN to develop and maintain international partnerships to detect, prosecute, and otherwise disrupt criminal activity facilitated by the illicit use of digital assets. As recently restated in the Anti-Money Laundering Act of 2020, FinCEN guidance has long stated that the BSA—the United States' primary AML/CFT statute—covers "value that substitutes for currency" (i.e., virtual currency) as it relates to money transmission and money transmitters.[75] A person, regardless of their location, doing business as a money transmitter wholly or in substantial part in the United States, such as by engaging in digital asset transactions with U.S. customers, must register as a Money Services Business (MSB) and comply with BSA/AML requirements.[76] Accordingly, in addition to the FATF framework described above, TFI has made significant investments in the following international partnerships:

Collaboration on Licensing and Supervision. Past coordination by Treasury with foreign financial regulators shows that such coordination can provide actionable intelligence to U.S. authorities as well as crucial information in cases to sanction these exchanges and their related individuals.

Trainings. Treasury and FinCEN have also undertaken training missions with international partners. These trainings have included sending instructors to countries that have active virtual currency marketplaces, yet need assistance from the U.S. government in understanding the implications of this industry for their existing regulatory and legal systems. These trainings provide overviews on what virtual currencies include and various industry models; how to prepare for an examination of a virtual currency exchanger; how to analyze transactions for the purpose of risk assessment and ongoing monitoring and KYC; suspicious transaction reporting; illicit finance trends in virtual currency; systems of software used to conduct transaction analysis; and how to research information on customers, wallets, and other topics through open-source research. Trainings are sometimes done in conjunction with presentations on risk assessments and the FATF standards by the Office of Terrorist Financing and Financial Crimes.

Internal Revenue Service-Criminal Investigation (IRS-CI)

IRS-CI investigates criminal violations of the U.S. Internal Revenue Code and other related financial crimes, including violations of the BSA and money-laundering prohibitions. Its Cybercrime Units (CCUs) have investigated, among other things, darknet vendors, ransomware actors, and digital currency money launderers, and have played an important role in improving the United States' relationships on cyber investigations with foreign law enforcement partners, including Europol. IRS-CI is establishing an Advanced Collaboration and Data Center (ACDC) to better track, share, and investigate the use of digital currencies in illicit activities, including unauthorized computer intrusions and human and drug trafficking. The ACDC will be a mission centric hub for specialized personnel, data and technology involving IRS-CI, other IRS components, Treasury, and partner agencies that provide both a common focus and value-added resource.

In June 2019, IRS-CI, in conjunction with the World Bank, hosted "Cyber NETwork 2019: Connecting Globally, Following the Money and Fighting Cybercrime," in Washington, DC. The event brought together over 100 representatives from more than 50 different countries around the world for an educational and intelligence sharing conference focusing on virtual currency, the dark web, open-source intelligence, and social media. In addition to case presentations and blockchain tracing sessions, the event offered a platform for participants to get a comprehensive look into the investigative activities associated with modern day financial fraud. Participants shared best practices to advance international collaboration and increase efforts in this area. The success of the 2019 summit has resulted in the planning of a second summit in the summer of 2022 in Washington, DC, where the World Bank will again partner with IRS-CI to host dozens of international partners to learn about current investigative techniques and present case studies about cryptocurrencies.

IRS-CI also sponsored a Cyber Summit in 2021 in Ireland that brought together cryptocurrency experts to assist with developing and conducting international cryptocurrency investigations. Students from the Irish Garda, Criminal Assets Bureau and Department of Revenue discussed tracking of digital assets, identifying co-conspirators, working with victims, working with foreign governments on formal and informal assistance, preparing for trial, and conducting seizures. After the training, the instructors and students remained in contact to support each other's cases and to leverage expertise to advance their investigations.

Finally, IRS-CI is participating in an action group with the Organization for Economic Cooperation and Development (OECD) Task Force on Tax Crimes to develop a FinTech Toolkit. This toolkit will help teach countries how to develop and conduct investigations involving illicit digital assets.

Department of Homeland Security

Immigration and Customs Enforcement, Homeland Security Investigations (HSI)

HSI is the largest international investigative presence in DHS and comprises 80 offices in over 50 countries. HSI focuses on expanding the borders out, leaning forward in the approach to identify and mitigate threats before they reach our borders. This multi-tiered, multi-pronged strategy is one which

spans international boundaries and crosses all investigative program areas. In 2011, HSI established the Transnational Criminal Investigative Unit (TCIU) Program, comprised of foreign law enforcement officials, customs officers, immigration officers, and prosecutors, to act as a force multiplier in the fight against TCOs. HSI TCIUs facilitate information exchange and rapid bilateral investigations involving violations within HSI's investigative authority and enhance the host country's ability to investigate and prosecute individuals involved in transnational criminal activity that threatens the stability and security of the region and, ultimately, U.S. homeland security. HSI special agents are uniquely positioned to partner with TCIU personnel to provide critical intelligence and resources to allow host country partners to take appropriate enforcement action under the authority of the host country. HSI works to combat the criminal exploitation of digital currencies through multiple units, including the Cyber Financial Section of the Financial Crimes Unit (FCU), which provides training to international partners and analytical assistance in tracing virtual currencies. HSI's Cyber Crimes Center (C3) has likewise led numerous digital asset trainings with foreign law enforcement partners.

Training and Outreach Efforts. HSI has developed a robust training and outreach program through three of the units that focus on investigations involving digital assets: FCU, which is charged with the oversight of all HSI financial investigations; C3; and the Asset Forfeiture Unit (AFU). 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 international law enforcement partners. To date in FY 2022, most trainings and outreach presentations have been conducted in person. This enables HSI headquarters units to provide comprehensive instruction into investigations that have any type of virtual currency nexus. In addition to in-person training, several presentations have been conducted virtually, thereby enabling HSI to reach other locations due to travel restrictions.

International trainings and outreach presentations since 2018 have included virtual and in-person trainings to law enforcement partners in Bangladesh, the Netherlands, Croatia, Latvia, Argentina, Switzerland, Colombia, France, Singapore, Egypt, Korea, Saudi Arabia, Panama, Mexico, Canada, Malaysia, El Salvador, and the Palestinian Authority:

Fiscal Year	In-Person Courses	Virtual Courses	Countries Participating	Total Students
2018	14	0	11	963
2019	10	0	6	869
2020	3	0	3	300
2021	0	11	5	826
2022	5	2	7	421

HSI is planning additional international training opportunities for FY 2022 in England, Jordan, the UAE, and Brazil.

United States Secret Service (USSS)

USSS investigates a variety of cybercriminal activity, including the illicit use of digital assets, by partnering with the global law enforcement community through both domestic field offices and 19 international attaché offices around the world. USSS prioritizes outreach, training, and education of international partners on cybercrime-related subjects. Through the U.S. Department of State's ILEAs, USSS trains foreign partners in numerous cybercrime-related subjects, including network intrusion response, digital forensics, and investigating cryptocurrency. USSS continues to support ILEAs located in Budapest, Hungary; Bangkok, Thailand; Gaborone, Botswana; San Salvador, El Salvador; Roswell, New Mexico; and the West African Regional Training Center in Accra, Ghana.

In addition to trainings conducted through the ILEAs, USSS also conducts direct outreach with international partners through its 19 attaché offices. Examples include:

- The Honolulu Field Office (HNL) covers the Hawaiian Islands, Oceania, and Asia through Pakistan, and oversees the Guam Resident Office, attaché offices in Bangkok and Hong Kong, a liaison to the Australian Federal Joint Police Cybercrime Center (JPC3), and a liaison to the Department of Defense U.S. Indo-Pacific Command. Since 2018, HNL has provided over 300 outreach events to a wide variety of foreign departments, including those located in Australia, New Zealand, Japan, Mongolia, Vietnam, Thailand, Singapore, Laos, Timor-Leste, Palau, and Nepal. Cryptocurrency seminars in India, Bangladesh, Maldives, the Philippines, Fiji, Palau, Papua New Guinea, and French Polynesia are in the scheduling phase for 2022.

- The Ottawa Field Office covers offices located in Vancouver and Montreal. The offices have provided numerous cyber-related outreach opportunities to Canadian law enforcement and private sector partners, including the Royal Canadian Mounted Police, the Canadian Anti-Fraud Centre, and the Bank of Canada.

- The Mexico City Resident Office (MEX) has offered the banking industry in Mexico (Mexican and U.S. banks) outreach on malicious cyber trends and best practices for cybersecurity. MEX is planning on conducting two engagements with the Mexican Attorney General's Office and the Mexican Financial Intelligence Unit (UIF) later in 2022 related to cybercrime.

- The Rome Field Office (ROM) covers 63 countries in Europe, Africa, and the Middle East, and oversees attaché offices in Sofia, Bulgaria, Pretoria, South Africa, and Bucharest, Romania. The Pretoria office has conducted numerous outreach events through in-person workshops and virtual seminars on cyber-related topics, including digital assets. ROM will assist with an international engagement on dark web investigations in both Vienna, Austria, and Rome later in 2022.

As COVID-19 restrictions continue to ease, USSS expects continued growth in the number of countries that participate in the USSS-taught ILEA investigative classes. The training efforts USSS has initiated with our foreign law enforcement partners are summarized in the chart:

Country and student participation in USSS-led ILEA investigative classes
October 2019 – March 2022

Fiscal Year	In-Person Courses	Virtual Courses	Countries Participating	Total Students
2019	13	0	56	373
2020	6	7	62	441
2021	5	4	35	223
2022	3	0	15	74

Securities and Exchange Commission

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).[77] The SEC's Office of International Affairs also has a technical assistance (TA) program that, among other things, assists foreign securities and regulatory authorities with enhancing their capital markets, building capacity, meeting international standards, and implementing best practices.

Securities statutes and regulations allow for the provision of effective TA to foreign counterparts, including in the digital assets area. Historically, SEC TA projects reach in the range of 1,600 to 2,000 foreign officials every year. With respect to digital assets, from the beginning of FY 2020 to the present, SEC staff have completed 17 TA projects, working with and training 334 foreign officials from more than 50 countries. Working with teams from OPDAT and the ICHIP program, SEC staff are currently planning two regional TA programs, for the American region (Mexico, Central and South America, and the Caribbean) and Southeast Asia, focused exclusively on digital assets. The American region program is tentatively scheduled for October 2022, with the Southeast Asia program to follow. In addition to foreign securities authorities, these programs are expected to include foreign banking and criminal law enforcement authorities, as well as FIUs. SEC TA staff were also scheduled to begin a 6-day program in May 2022 for the African region covering digital assets and related topics. Representatives from securities and regulatory authorities, FIUs, criminal prosecutorial agencies, and securities exchanges are expected to attend.

Commodity Futures Trading Commission

International commodity and derivative exchanges are increasingly requesting the CFTC's expertise in dealing with market structure and oversight, supervisory oversight, enforcement strategies and corporate governance. The CFTC's Office of International Affairs' Technical Assistance (TA) program leverages the expertise of CFTC staff and industry officials to provide training and support to the global regulatory community. The aim of the TA program is to help improve market development, enhance supervisory coordination and cooperation in an ever increasing global, interwoven marketplace, and enhance the enforcement capacity of regulators around the world. This is done through international conferences, regulatory assessments and gap analysis, study tours with regulators and industry participants, training, and other means of technical support.

The CFTC's TA program provides assistance to over 1,500 foreign officials from over 100 jurisdictions on an annual basis. Commodity and derivative markets are no longer location sensitive, and market disruptions in one part of the world often have an adverse impact in another part of the world. As part of the global regulatory community, the CFTC works with colleagues around the world to enhance the oversight of global markets and improve transparency; increase global financial market stability and resiliency; support commodity and derivative exchanges in developing countries to further economic development and provide a viable means of hedging risk and bringing products to the global market; and foster closer cooperation in international enforcement efforts. The CFTC's TA program has led over a dozen trainings involving digital asset derivatives and digital asset commodities in the past two years; and is closely coordinated with similar programs from other domestic and international agencies including the SEC, Treasury, and the United States Agency for International Development (USAID), as well as other similar programs conducted by third parties, such as the International Monetary Fund, World Bank, International Organization of Securities Commissions (IOSCO), and Financial Services Volunteer Corp.

---

[1] The term "digital assets" used throughout this Report comports with the definition in the Executive Order. *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.").

[2] As defined in the Executive Order, "[t]he term 'cryptocurrencies' refers to 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." Exec. Order No. 14067, 87 Fed. Reg. at 14151 (Sec. 9(c)). A full description of blockchain technology is beyond the scope of this Report, but basic information

about cryptocurrency transactions is provided in the U.S. Dep't of Just., Report of the Attorney General's Cyber Digital Task Force: *Cryptocurrency Enforcement Framework*, at 2-4 (2020) [hereinafter *Cryptocurrency Enforcement Framework*], https://www.justice.gov/archives/ag/page/file/1326061/download.

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

[4] S*ee Cryptocurrency Enforcement Framework, supra* note 2.

[5] *See, e.g., Cryptocurrency Enforcement Framework, supra*, note 2, at 15-16.

[6] *See* Exec. Order No. 14067, 87 Fed. Reg. at 14144 (Sec. 2(c)).

[7] The descriptions of digital assets herein generally apply to digital assets that use permissionless blockchains (also known as trustless or public blockchains), which are public and open networks that allow any individual to use them, the most common of which is Bitcoin.

[8] Bitcoin is both a cryptocurrency and a protocol; because of this, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the currency.

[9] The Financial Action Task Force (FATF) defines "virtual asset" as a "digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes." Financial Action Task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Oct. 2021) [hereinafter FATF 2021 *Guidance*], at 21, 109, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf. "Virtual assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations." *Id*. at 21-22, 109. The FATF defines "virtual asset service provider" as any natural or legal person that as a business conducts one or 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. *Id*. at 22, 109. Although the terms "virtual asset" and "digital asset" can be used interchangeably, "digital asset" is the preferred term used throughout this Report consistent with Exec. Order No. 14067. The term "virtual asset" is used when discussing FATF-related language.

[10] The Convention on Cybercrime of the Council of Europe, also known as the Budapest Convention on Cybercrime or the Budapest Convention, is the first international treaty on crimes committed via the Internet and other computer networks, and whose main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation. *See* Council of Europe, *Convention on Cybercrime,* Nov. 23, 2001, Europ. T.S. No. 185, pmbl. *available at* https://rm.coe.int/1680081561. *See also* Council of Europe, Details of Treaty No. 185, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185. The Department of Justice and Department of State are working actively to promote the Budapest Convention and grow its membership, which is a critical tool for international cooperation in all types of investigations. In May 2022, the United States signed the Second Additional Protocol to the Budapest Convention, which aims to further

enhance cooperation on cybercrime and electronic evidence sharing through more efficient mutual assistance tools and other forms of cooperation between countries, cooperation in emergencies, and direct cooperation between law enforcement in one country and service providers and other private entities in another country.

[11] Letters rogatory are the usual means of obtaining judicial assistance from overseas in the absence of a treaty or other agreement. *See* U.S. Dep't of State, *Preparation of Letters Rogatory,* https://travel.state.gov/content/travel/en/legal/travel-legal-considerations/internl-judicial-asst/obtaining-evidence/Preparation-Letters-Rogatory.html. Compliance with such requests is voluntary.

[12] For purposes of OFAC sanctions programs, the Department of Treasury defines "virtual currency" as "a digital representation of value that functions as (i) a medium of exchange; (ii) a unit of account; and/or (iii) a store of value; and is neither issued nor guaranteed by any jurisdiction." U.S. Dep't of Treasury, *Frequently Asked Questions on Virtual Currency,* https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1626. Virtual currency is a subset of digital assets and includes cryptocurrencies and tokens issued by private organizations.

[13] U.S. Dep't of Justice, Criminal Division, *Global Cyber and Intellectual Property Crimes,* https://www.justice.gov/criminal-opdat/global-cyber-and-intellectual-property-crimes.

[14] U.S. Dep't of Treasury, 2022 *National Money Laundering Risk Assessment, supra* note 3 at 41.

[15] *FATF 2021 Guidance, supra* note 9 at 55-57.

[16] *Id*. at 55-60, 82.

[17] Outside of the IOSCO framework, the SEC has entered into nine bilateral technical-assistance specific MOUs, and approximately two-dozen bilateral enforcement MOUs that can extend to technical assistance. *See* SEC, *Cooperative Arrangements with Foreign Regulators,* https://www.sec.gov/about/offices/oia/oia_cooparrangements.shtml. The CFTC likewise provides and receives cooperation from its foreign regulatory counterparts through formal and informal arrangements outside of the IOSCO MMoU framework, including with investigations involving digital assets.

[18] 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.

[19] U.S. Dep't of Treasury, *Sanctions Compliance Guidance for the Virtual Currency Industry* (October 2021), https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf.

[20] *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 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.

[21] *See, e.g.,* Posture Statement of General Paul M. Nakasone, Commander, United States Cyber Command, Before the 117th Congress Senate Committee on Armed Services (Apr. 5, 2022), https://www.cybercom.mil/Media/News/Article/2989087/posture-statement-of-gen-paul-m-nakasone-commander-us-cyber-command-before-the/

[22] Pursuant to Section 801 of the Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, 110 Stat. 1214 (codified at 28 U.S.C. § 509 (note)), "[t]he Attorney General and the Secretary of the Treasury are authorized to support law enforcement training activities in foreign countries, in consultation with the Secretary of State, for the purpose of improving the effectiveness of the United States in investigating and prosecuting transnational offenses." That statutory purpose can be accomplished either by direct funding to the Department of Justice from Congress, or by Foreign Assistance Act funding from the Department of State to the Department of Justice.

[23] FATF, *Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers* at 10-11, 14 (July 2021), https://www.fatfgafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf.

[24] *Id*. at 2, 19.

[25] Chainalysis, *The 2022 Crypto Crime Report* at 11 (Feb. 2022). The estimate in the cited report is conservative because it takes into account only funds derived from what the company calls "cryptocurrency-native crime," which it describes as "cybercriminal activity such as darknet market sales or ransomware attacks in which profits are virtually always derived in cryptocurrency." *Id*. Chainalysis acknowledges that "fiat currency derived from offline crimes" such as drug trafficking is also "converted into cryptocurrency to be laundered," but provides no estimate on the amount of such funds because it is "more difficult to measure." *Id*.

[26] Elliptic, *Typologies Report 2022 - Preventing Financial Crime in Cryptoassets.pdf,* at 120.

[27] Blockchain analysis firm Chainalysis estimated more than $692 million ransomware payments made in 2020—nearly double the amount the firm initially estimated at the same time the year before. Chainalysis, *The 2022 Crypto Crime Report, supra* n.25 at 38.

[28] 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.

[29] Press Release, *Ukrainian Arrested and Charged with Ransomware Attack on Kaseya, U.S. Dep't of Justice* (Nov. 8, 2021), https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya.

[30] *See, e.g.,* MacKenzie Sigalos, *Crypto scammers took a record $14 billion in 2021,* CNBC, Jan. 6, 2022, https://www.cnbc.com/2022/01/06/crypto-scammers-took-a-record-14-billion-in-2021-chainalysis.html. *See also* Chainalysis, *The 2022 Crypto Crime Report, supra* note 25, at 5-6 ($7.8 billion taken from victims in scams, and $3.2 billion stolen through cryptocurrency theft).

[31] Sigalos, *supra* note 30.

[32] U.S. Dep't of Treasury, *2022 National Money Laundering Risk Assessment, supra* note 3 at 42.

[33] *See* Federal Bureau of Investigation, *Internet Crime Report 2021,* at 12-13, https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf. *See also* Mengpi Sun, *Pandemic, Crypto Fuel Increase in Romance Scams,* WALL ST. J. (Feb. 14, 2022), https://www.wsj.com/articles/pandemic-crypto-fuel-increase-in-romance-scams-11644879123.

[34] FBI, Internet Crime Report 2021, *supra* note 33 at 12-13.

[35] Chainalysis, *The 2022 Crypto Crime Report, supra* note 25 at 5.

[36] Press Release, *U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats, supra* note 18.

[37] Rebecca S. Portnoff, et. al, *Backpage and Bitcoin: Uncovering Human Traffickers,* KDD '17: PROCEEDINGS OF THE 23RD ACM SIGKDD INTERNATIONAL CONFERENCE ON KNOWLEDGE DISCOVERY AND DATA MINING, August 2017, at 1597, *available* at https://www.kdd.org/kdd2017/papers/view/backpage-and-bitcoin-uncovering-human-traffickers.

[38] *Cryptocurrency Enforcement Framework, supra* note 2 at 7.

[39] *Id*. at 11 (describing allegations in civil-forfeiture complaint against the al-Qassam Brigades).

[40] U.S. Dep't of Treasury, *Frequently Asked Questions on Virtual Currency, supra* note 12.

[41] Press Release, *Russian National and Bitcoin Exchange Charged In 21-Count Indictment for Operating Alleged International Money Laundering Scheme and Allegedly Laundering Funds from Hack of Mt. Gox,* U.S. Dep't of Justice (July 26, 2017), https://www.justice.gov/usaondca/pr/russian-national-and-bitcoin-exchangecharged-21-count-indictment-operating-alleged. *See also* Press Release, *FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales,* Financial Crimes Enforcement Network (Jul. 27, 2017), https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware.

[42] For other examples of cases in which virtual currency exchanges have been charged with operating an unlicensed money transmitting business, *see United States v. Murgio,* No. 15-769 (AJN), 2017 WL 365496 (S.D.N.Y. Jan. 20, 2017) and *United States v. Faiella,* 39 F. Supp. 3d 544 (S.D.N.Y. 2014). *See also United States v. Budovsky,* No. 13-368 (DLC), 2015 WL 5602853, at *14 (S.D.N.Y. Sept. 23, 2015) (noting that 18 U.S.C. § 1960, which covers operation of an unlicensed money transmitting business, encompasses businesses that transmit virtual currency).

[43] 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.

[44] Press Release, *First Bitcoin "Mixer" Penalized by FinCEN for Violating Anti-Money Laundering Laws,* Financial Crimes Enforcement Network (Oct. 19, 2020), https://www.fincen.gov/news/news-releases/first-bitcoin-mixer-penalized-fincen-violating-anti-money-laundering-laws.

[45] 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.

[46] The only form of payment accepted on Silk Road was bitcoin. Upon registering an account with Silk Road, users were assigned a Bitcoin address. Bitcoin sent to the user's Bitcoin address was credited to the user's account. All told, Silk Road generated sales revenue totaling over 9.5 million BTC, and collected commissions from these sales totaling over 600,000 BTC. The figures were, at the time of Ulbricht's initial charges by complaint, equivalent to approximately $1.2 billion USD in sales and approximately $80 million USD in commissions.

[47] Verified Complaint for Forfeiture In Rem, *United States v. Cazes,* No. 1:17-at-00557, at 21 (E.D. Cal. July 19, 2017), *available at,* https:// www.justice.gov/opa/press-release/file/982821/ download.

[48] Press Release, *AlphaBay, the Largest Online "Dark Market," Shut Down,* U.S. Dep't of Justice (July 20, 2017), https://www.justice. gov/opa/pr/alphabay-largest-online-darkmarket-shut-down.

[49] Press Release, *Dark Web Administrator Sentenced to 20 Years in Prison for Narcotics Trafficking and Money Laundering,* U.S. Dep't of Justice (Oct. 9, 2018), https://www.justice.gov/opa/pr/dark-web-administrator-sentenced-20-years-prison-narcotics-trafficking-and-money-laundering.

[50] Press Release, *3 Germans Who Allegedly Operated Dark Web Marketplace with Over 1 Million Users Face U.S. Narcotics and Money Laundering Charges,* U.S. Dep't of Justice (May 3, 2019), https://www.justice.gov/usao-cdca/pr/3-germans-who-allegedly-operated-dark-web-marketplace-over-1-million-users-face-us.

[51] Exit scams are common among large dark-net marketplaces, which typically hold money in escrow while a vendor delivers illicit goods.

[52] Press Release, *South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin,* U.S. Dep't of Justice (Oct. 16, 2019), https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-otherscharged-worldwide-takedown-largest-darknetchild.

[53] Press Release, *International Law Enforcement Operation Targeting Opioid Traffickers on the Darknet Results in over 170 Arrests Worldwide and the Seizure of Weapons, Drugs and over $6.5 Million,* U.S. Dep't of Justice (Sept. 22, 2020), https://www.justice.gov/opa/pr/international-law-enforcement-operation-targeting-opioid-traffickers-darknet-results-over-170.

[54] Press Release, *Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace*, U.S. Dep't of Justice (April 5, 2022), https://www.justice.gov/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace.

[55] Financial Crimes Enforcement Network, "FinCEN Alerts Financial Institutions to Convertible Virtual Currency Scam Involving Twitter," July 16, 2020, https://www.fincen.gov/sites/default/files/2020-07/FinCEN%20Alert%20Twitter_508%20FINAL.pdf.

[56] Press Release, *Three Individuals Charged for Alleged Roles in Twitter Hack,* U.S. Dep't of Justice, (July 31, 2020), https://www.justice.gov/usao-ndca/pr/three-individuals-charged-alleged-roles-twitter-hack. *See also* Press Release, *Man Arrested in Connection with Alleged Role in Twitter Hack,* U.S. Dep't of Justice (July 21, 2021), https://www.justice.gov/opa/pr/man-arrested-connection-alleged-role-twitter-hack.

[57] These included Europol and Eurojust, which were an integral part of coordination. Investigators and prosecutors from several jurisdictions, including Romania's National Police and the Directorate for Investigating Organised Crime and Terrorism; Canada's Royal Canadian Mounted Police; France's Court of Paris and BL2C (anti-cybercrime unit police); the Dutch National Police; Poland's National Prosecutor's Office, Border Guard, Internal Security Agency, and Ministry of Justice; and the governments of Norway and Australia provided valuable assistance. Germany's Public Prosecutor's Office Stuttgart and State Office of Criminal Investigation of Baden-Wuerttemberg; Switzerland's Public Prosecutor's Office II of the Canton of Zürich and Cantonal Police Zürich; the National Police of Ukraine and the Prosecutor General's Office of Ukraine; and the United Kingdom's National Crime Agency also provided significant assistance.

[58] Press Release, *Director and Promoter of BitConnect Pleads Guilty in Global $2 Billion Cryptocurrency Scheme,* U.S. Dep't of Justice (Sept. 21, 2021), https://www.justice.gov/usao-sdca/page/file/1431236/download.

[59] Press Release, *Almost $57 Million in Seized Cryptocurrency Being Sold for Victims of BitConnect Fraud,* U.S. Dep't of Justice (Nov. 16, 2021), https://www.justice.gov/usao-sdca/pr/almost-57-million-seized-cryptocurrency-being-sold-victims-bitconnect-fraud.

[60] Press Release, *Treasury Takes Robust Actions to Counter Ransomware,* U.S. Dep't of Treasury (Sept. 21, 2021), https://home.treasury.gov/news/press-releases/jy0364.

[61] U.S. Dep't of 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.

[62] 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. 18, 2021), https://home.treasury.gov/news/press-releases/jy0471.

[63] *Id.*

[64] 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 (April 5, 2022), https://home.treasury.gov/news/press-releases/jy0701.

[65] For a list of SEC crypto assets and cyber enforcement actions, see https://www.sec.gov/spotlight/cybersecurity-enforcement-actions.

[66] *See* Press Release, *Defendants Charged in Fraudulent ICO to Pay Nearly $7 Million, Litigation Release No. 24635, Securities and Exchange Commission v. PlexiCorps, Dominic Lacrois, and Sabrina Paradis-Royer, No. 1:17-cv-0770-CBA-RML (E.D.N.Y.),* SEC (Oct. 2, 2019), https://www.sec.gov/litigation/litreleases/2019/lr24635.htm.

[67] In the context of pursuing violations of the U.S. securities laws in the crypto-asset space, at least one defendant has challenged the SEC's authorities to use voluntary cross-border cooperation agreements to obtain evidence during the pendency of litigation. In rejecting that challenge, a magistrate judge in the Southern District of New York noted the SEC's viewpoint that "this cross-border cooperation is critical to its mission of protecting the investing public and maintaining fair and transparent global market," and "conclude[d] that the SEC's use of [foreign requests for assistance] is permissible and not an af[f]ront to the Court's jurisdiction." *SEC v. Ripple Labs, Inc.,* 540 F. Supp. 3d 409, 411 (S.D.N.Y. 2021).

[68] As part of that regulatory authority, the CFTC designates contract markets or registered swap execution facilities that offer derivatives on digital assets to U.S. customers.

[69] In the past four years, the CFTC has brought two dozen cases involving some sort of fraud connected with digital assets. 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.

[70] *See* 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.

[71] *See* 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.

[72] *See* Press Release, *CFTC Charges Two Individuals with Multi-Million Dollar Digital Asset Pump-and-Dump Scheme,* CFTC (Mar. 5, 2021), https://www.cftc.gov/PressRoom/PressReleases/8366-21.

[73] 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.

[74] TCOs use cryptocurrency to not only facilitate drug transactions on darknet markets, but also to launder drug proceeds across international borders. As worldwide border restrictions and travel bans imposed as a result of the COVID-19 pandemic complicated bulk cash smuggling operations, TCOs increasingly turned to cryptocurrency as a means to quickly, efficiently, and anonymously move drug proceeds from the United States to countries abroad.

[75] *See* 31 U.S.C. §§ 5312(a), 5330(d). That is consistent with FinCEN's 2011 MSB Final Rule, 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); in particular, see 31 C.F.R. § 1010.100(ff)(5)(i)(A).

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

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