Jeremy Sheridan
Assistant Director
Office of Investigations
United States Secret Service

Prepared Testimony

Before the
United States House of Representatives
Committee on Homeland Security
Subcommittee on Intelligence and Counterterrorism
July 22, 2021

Introduction

Good morning Chairwoman Slotkin, Ranking Member Pfluger, and members of this Subcommittee: Thank you for inviting me to testify on how criminals use digital money,[1] including cryptocurrencies, to further illicit activity, such as terrorism and unlawful acts of violent extremism. My name is Jeremy Sheridan and I am the Assistant Director of the Office of Investigations. In this role, I lead more than 160 Secret Service field offices and direct our network of Cyber Fraud Task Forces (CFTFs) in their investigations of sophisticated computer and financial crimes. I ensure our global network of field offices and task forces effectively detect and arrest those that are engaging in the criminal violations we are authorized to investigate,[2] while fully supporting our diverse protective requirements across the world.

Today, I will provide you with an overview of the risks associated with digital money, as viewed from the perspective of the United States Secret Service (Secret Service), and to highlight the various actions we are taking to address those risks. As part of my testimony, I will also seek to highlight some key challenges that we see on the horizon.

For more than 150 years, the Secret Service has conducted investigations to protect the American public, private companies, financial institutions, and critical infrastructure from criminal exploitation. We maintain extensive authorities, expertise, and capabilities to effectively safeguard financial and payment systems from criminal misuse, even as those illicit activities are increasingly transnational in nature and enabled by the Internet.[3]

The Secret Service has a distinctive record of success in countering risks related to emerging financial and payment technologies. This includes countering fraud in electronic transfers of funds in the early 1980s, countering criminal schemes related to payment cards in the 1990s, and investigations related to cryptocurrencies and digital money platforms over the past decade and half. Today, we remain committed to keeping pace with technological innovation and the evolving strategies and tactics criminals are using to exploit these new financial instruments.

Through our decades of criminal investigations, the Secret Service has developed a deep understanding of the risks, challenges, and potential investigative benefits of digital money, as well as the effectiveness of various potential law enforcement and regulatory responses. Our perspective on these matters is based on our unique role. We are not a financial regulator or a member of the intelligence community. We are a law enforcement agency focused on accomplishing our dual responsibilities of protecting designated persons, places, and events and investigating crimes that undermine the integrity of financial and payment

[1] The term "digital money" is used to refer to a representation of value that is stored on and transferred through computer systems and that is used similar to money, regardless of legal tender status. The term "digital money" is inclusive of, but is not limited to, cryptocurrency assets like Bitcoin, Ether, Tether, and others. Consistent with FinCEN guidance (FIN-2013-G001), the Secret Service uses the term "virtual currency" to refer to mediums of exchange that operate like currency, but do not have legal tender status.
[2] *See* 18 U.S.C. §§ 1028-1030, and 3056(b).
[3] For more information on the Secret Service's investigative mission see: https://www.secretservice.gov/investigation

systems. These unified mission sets necessitate that we understand how digital money may present risks our nation's financial system, such as through money laundering, fraud, theft, and extortion by cyber criminals (including through ransomware), in addition to the ways in which they present risks to our many protectees.

Consequently, my testimony today will address the broad risks of how criminals can use digital money. In the interest of protecting ongoing investigative activities and other law enforcement sensitive information, I will avoid detailed discussion of specific recent events or law enforcement techniques. I believe this committee's work can be well informed by a discussion of the broad range of illicit activity that is enabled by digital money. The measures to investigate and address these risks, I believe, apply equally to terrorism, violent extremism, and financially motivated crime, as they do to other forms of criminality.

Secret Service Investigations of Digital Money

The commercialization of the Internet in the 1990s brought with it a new push to develop payment systems that could function effectively within a digital economy. While the U.S. market predominately adopted payment cards as the solution, there have been numerous attempts to develop new digital payment systems that could operate with greater independence from, and with a similar degree of trust to, the traditional financial system, and all at a potentially lower cost. In 2009, Bitcoin sought to achieve these goals through a novel approach of using public-key cryptography and ongoing decentralized computation to form a blockchain, a technical architecture which forms the basis of most forms of digital money today.[4]

Since that time, the popularity of Bitcoin has inspired an exponential growth in digital assets globally, from cryptocurrencies to stable coins to non-fungible tokens (NFTs). As of July 2021, there are more than 5,000 blockchains in operation on the Internet, with over 300 million users worldwide and total market capitalization of approximately $1.43 trillion.[5] Even central banks are exploring these technologies as a means of encouraging more transparent and seamless financial exchanges. Several are already in circulation.[6] While much of this effort is in support of legitimate economic activity, the rapid expansion of cryptocurrencies, as well as other digital stores of value, presents a significant challenge to law enforcement, and a growing area of risk to the U.S. and our foreign partners.

The Secret Service has been at the forefront of combatting these crimes from their earliest iterations, and we continue this work today. We have successfully investigated and dismantled two centralized virtual

[4] Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008). Last accessed on July 6, 2021. Available at: https://bitcoin.org/bitcoin.pdf

[5] "Cryptocurrency Prices by Market Cap," Last accessed on July 6, 2021. Available at: https://www.coingecko.com/en.

[6] Among others, the Central Bank of Sweden proposed an "e-krona" in November 2016, and started testing an e-krona proof of concept in 2020; in November 2017, the Central Bank of Uruguay announced to begin a test to issue digital Uruguayan pesos; and on October 20, 2020, the Central Bank of the Bahamas introduced the "Sand Dollar" as a digital legal currency equivalent to the traditional Bahamian dollar. See Deloitte, "Are Central Bank Digital Currencies (CBDCs) the money of tomorrow?" Last accessed on July 11, 2021. Available at https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/Banking/lu-are-central-bank-digital-currencies.pdf

currency providers that supported extensive criminal activity: e-Gold Ltd. (in 2007)[7] and Liberty Reserve (in 2013).[8] Working with our partners, we investigated and ultimately shutdown a number of other virtual currency exchangers,[9] including Western Express, [10] which was prosecuted by the Manhattan District Attorney's Office, and, in 2017, the cryptocurrency exchange BTC-e.[11] Through a partnership with the Internal Revenue Service's Criminal Investigation Division (IRS-CI) and other foreign and domestic law enforcement agencies, we successfully shuttered BTC-e, after it was accused to have failed to implement a program to prevent illicit financing.[12]

More recently, in collaboration with our federal and international partners, we successfully investigated a highly sophisticated, Russia-based criminal scheme to defraud multiple cryptocurrency exchangers and their customers. [13] This effort led to the seizure of millions of dollars' worth of virtual assets. The criminals indicted in this scheme are alleged to have employed a variety of advanced methods in support of their fraud, including using fictitious or stolen identities to create accounts; circumventing exchanges' internal controls; swapping and mixing different types of virtual currency; moving virtual currency through multiple intermediary addresses; and a market manipulation scheme in which inexpensive virtual currency was purchased at a fast rate to increase demand and price, then quickly sold for a higher price to make a quick profit.

And just this year, our work investigating illicit uses of cryptocurrency supported indictments and arrests associated with a vast money laundering operation that provided criminal services to not only some of the

[7] *See* U.S. Department of Justice: "Over $56.6 Million Forfeited In E-Gold Accounts Involved In Criminal Offenses," https://www.justice.gov/usao-md/pr/over-566-million-forfeited-e-gold-accounts-involved-criminal-offenses; Digital Currency Business E-Gold Indicted for Money Laundering and Illegal Money Transmitting, https://www.justice.gov/archive/opa/pr/2007/April/07_crm_301.html.

[8] *See* U.S. Department of Justice press releases: "Founder of Liberty Reserve Pleads Guilty to Laundering More Than $250 Million through His Digital Currency Business," https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital; "Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One Of World's Largest Digital Currency Companies, And Seven Of Its Principals And Employees For Allegedly Running A $6 Billion Money Laundering Scheme," https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-liberty-reserve-one-world-s-largest.

[9] Exchangers are businesses that allow for the trade of digital currencies for other assets, such as conventional fiat money, such as US dollars, or other digital currencies.

[10] *See* Manhattan District Attorney, "DA Vance Testimony on Digital Currency before the Department of Financial Services," https://www.manhattanda.org/da-vance-testimony-on-digital-currency-before-the-department-of-financial-services/.

[11] *See,* "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," https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged."

[12] See, "FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales" https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware.

[13] *See*, "Russian Nationals Indicted for Conspiracy to Defraud Multiple Cryptocurrency Exchanges and Their Customers," https://www.justice.gov/usao-ndca/pr/russian-nationals-indicted-conspiracy-defraud-multiple-cryptocurrency-exchanges-and ; "Treasury Sanctions Russian Cyber Actors for Virtual Currency Theft," https://home.treasury.gov/news/press-releases/sm1123.

world's most dangerous cybercriminals but also North Korean military-affiliated actors.[14] This North Korean group is accused of creating and deploying multiple malicious cryptocurrency applications, of developing and fraudulently marketing a fictitious blockchain platform, and ultimately stealing more than $1.3 billion from victims in the United States and overseas.

During the course of our criminal investigations, the Secret Service maintains close and continuous partnerships with a wide range of domestic and international law enforcement agencies. We regularly coordinate our work with the Department of Justice, Federal Bureau of Investigation (FBI), Homeland Security Investigations (HSI), IRS-CI and others, and, where appropriate, conduct joint-investigations and information sharing with foreign counterparts. Through our Cyber Fraud Task Forces and through domestic and international task forces, like the National Cyber Investigative Joint Task Force (NCIJTF) and the Joint Cybercrime Action Taskforce (J-CAT) in Europe, we work to ensure effective deconfliction and intelligence sharing between and among our law enforcement partners.

Countering Risks Involving Digital Money

Criminals can abuse digital money for a wide variety of purposes, including in support of terrorist or violent extremist activities. The types of criminality are diverse, and include such schemes as crypto-jacking,[15] thefts of private keys,[16] the purchase of illicit goods or services on the darkweb, attacks on block chain networks,[17] money-laundering, sanctions evasion, illicit financing, and as the extortion payment method of choice in modern ransomware, among other potential crimes.[18]

The blockchain analysis tracking firm Chainalysis, has identified approximately $21.4 billion worth of likely illicit cryptocurrency transfers in 2020.[19] However, we believe that this is likely a significant underestimate of the total value of illicit cryptocurrency transfers. Certain blockchain implementations on specific currencies can provide information for insightful analysis on its own, but a full accounting of the motives and identities of criminal actors using these tools can only be achieved through the work of trained criminal investigators, armed with subpoena powers and court-sanctioned legal process to undercover the true scale of the problem.

---

[14] *See*, "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and

[15] Crypto-jacking is the use of malware or compromised websites to use, without authorization, computing power of others for cryptocurrency mining. Mining is the computational process that verifies and maintains a blockchain, and is typically incentivized by a blockchain protocol rewarding cryptocurrency to miners.

[16] Control of assets on a blockchain is maintained through exclusive control and access to the associated private cryptographic key; however, there have been numerous instances of cryptocurrency heists, involving major exchanges, wallets, and individual users resulting from the theft and illicit use of private cryptographic keys.

[17] We have observed a few instances of attacks on blockchain systems themselves, either to impair their operation, as part of a broader scheme, or as part of a "51% attack" to defraud other users of the cryptocurrency. Such activities typically involve violations of 18 U.S.C. § 1030 and can also include other criminal offenses.

[18] Ransomware, which impairs the operation of a computer as part of an extortion demand, has substantially grown in threat, corresponding with adopting cryptocurrencies as the means of paying extortion demands.

[19] "Crypto Crime Report 2021," Chainalysis, available at: https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf.

A 2019 study[20] on terrorist use of digital currencies by the RAND Corporation, supported Secret Service's Office of Investigations finding that a specific digital currency can be viewed as more or less appealing to bad actors based upon six criteria: a currency's level of *anonymity*, its *usability*, its *security*, its *acceptance* in the marketplace, its *reliability*, and its overall *volume*. RAND's research shows that, "should a single cryptocurrency emerge that provides widespread adoption, better anonymity, improved security, and that is subject to lax or inconsistent regulation, then the potential utility of this cryptocurrency, as well as the potential for its use by terrorist [or criminal] organizations, would increase." It is thus essential that the U.S. Government keep pace with changes in the market and align investigative resources and regulatory oversight to shifts in the tactics of terrorists, criminals, and other bad actors.

Law enforcement has made tremendous strides in the fight against illicit use of digital money, but we anticipate that the ongoing growth in criminality will continue in the coming years. Organized crime groups, terrorists, violent extremists, and other bad actors will continue to view cryptocurrencies as an effective means to transfer substantial values globally, without encountering the anti-money laundering controls common in the traditional financial system. As the cryptocurrency industry improves their compliance with anti-money laundering (AML) obligations, I am focused on keeping the Secret Service one step-ahead of our adversaries. By developing the investigative capabilities and purview to meet the evolving threat landscape, we can continue to detect and arrest those engaged in crime, including those engaged in terrorism and violent extremism.

Challenges for Further Consideration

Cryptocurrencies remain attractive to bad actors for the various reasons provided above, but it also has its limitations and criminal drawbacks. For cryptocurrencies or other digital assets to be utilized within the mainstream economy – namely, to exchange them for most goods or services – they usually must be converted into government-backed fiat currency, such as the U.S. dollar, European euro, or Chinese yuan. This conversion typically occurs through "exchanges," money services businesses which allow for the purchase and sale of digital assets with fiat currency. Exchanges, both as on-ramps and off-ramps to the cryptocurrency economy, have been a particularly effective data source and control point for governments to focus their efforts; however, as the variety of digital assets increases, further attention is needed to address the risks of technologies and services that obscure digital transactions from law enforcement and regulatory oversight.

The United States and the broader international community have spent decades developing, implementing, and strengthening a global anti-money laundering (AML), Know-Your-Customer (KYC), and countering the financing of terrorism (CFT) regime. Financial institutions doing business in the United States must follow a host of statutory and regulatory obligations, including those related to the Bank Secrecy Act of 1970, the Annunzio-Wylie Anti-Money Laundering Act of 1992, and the Money Laundering Suppression Act of 1994, in addition to other associated laws and Federal regulations. These laws require covered entities to be registered, establish compliance programs, due diligence systems and monitoring programs, transmit suspicious activity reports, and develop risk-based anti-money laundering programs. Failing to comply with these requirements or conducting or facilitating transactions designed to

[20] *See*, "Terrorist Use of Cryptocurrencies Technical and Organizational Barriers and Future Threats," The RAND Corporation, 2019, available at https://www.rand.org/pubs/research_reports/RR3026.html.

avoid reporting requirements or conceal or promote specified unlawful activities may constitute criminal violations of Title 31 of the U.S. Code or sections 1956, 1957, or 1960 of Title 18, in addition to other provisions of U.S. law.

Criminals and terrorist groups persistently seek to avoid U.S. and foreign AML and KYC requirements by utilizing exchanges that do not adhere to these laws or reporting requirements. Criminals are also increasingly exploiting over-the-counter (OTC) brokers, which facilitate transactions conducted directly between two parties through bilateral contracts. Unlicensed OTC brokers with weak AML/CFT programs are increasingly being used by criminals and other bad actors for money laundering and other financial crimes. Compared to institutional exchanges, OTC brokers provide a more decentralized approach, which makes them attractive for those intent on engaging in money laundering activity. In both cases, with exchanges or OTCs, criminals look to utilize those providers hosted in foreign jurisdictions with lax AML requirements or weak enforcement.

Accordingly, it is vital to U.S. national security that AML/KYC laws achieve their intended effects, regardless of the bad actors' motivations for exploiting them. The enactment of the Anti-Money Laundering Act of 2020 (AML 2020) was an important step in this direction. Timely and effective implementation of the rules directed by this law, and effective enforcement of violations, will likely have a substantial impact on the illicit market.

We are closely monitoring and participating in the implementation of the AML Act of 2020, both to track potential emerging risks and to identify where further action may be helpful. For example, enhanced data reporting, collection, retention requirements, and accessibility requirements may strengthen criminal investigations and effective oversight. We also foresee significant money laundering risks, which may require further action, related to anonymity-enhanced cryptocurrencies, services intended to obscure transactions on blockchains (i.e., cryptocurrency tumblers or mixers), and cryptocurrency mining pools.

That said, the United States should be cautious about acting unilaterally, as this can simply lead to the "offshoring" of cryptocurrencies and associated services to foreign jurisdictions. We believe that the most effective interventions are those that are conducted in coordination with other major economic powers. Our foreign partners perform critical roles in in assisting U.S. law enforcement with conducting investigations, making arrests, seizing criminal assets, and establishing effective AML regulations to counter transnational criminal activity that harms Americans. As we take steps domestically, we continue to work to ensure that foreign partners are willing and capable to assist us in investigations. To that end, the Secret Service continues to partner closely with Departments of State, Justice, and the Treasury to develop these essential foreign partnerships and work collaboratively on multinational criminal investigations and training programs.

Further, we acknowledge that some exchangers or brokers may actively obfuscate their ownership and location in an effort to evade detection and oversight. To address this challenge, additional consideration is warranted to improve cooperation between U.S. government authorities and foreign and domestic providers of electronic communications services and remote computing services. This will facilitate expeditiously identifying users engaged in certain illicit activities, such as those involving digital money

laundering, transnational cybercrime, or terrorist financing. Last year, the Cyberspace Solarium Commission made important recommendations towards achieving such improved cooperation.[21]

Strong overseas partnerships are also key to effective regulation and oversight. Fostering these partnerships requires continual investment in government-to-government law enforcement and regulatory relationships to develop shared understanding of risks, and to ensure an effective international anti-money laundering regulatory and enforcement programs. Towards this end, we welcome efforts to improve global controls related to digital assets, through our international partners, and other global financial and banking associations.

Finally, investigating crimes involving digital money, and the transnational organized criminal and terrorist groups that exploit it, requires highly skilled criminal investigators. Hiring, developing, retaining, and equipping our investigative workforce, as well as partnering with and training our domestic and foreign law enforcement and other partners to develop their investigative capabilities, are all critical priorities for ensuring that the United States is well prepared to address emerging risks both today and into the future.

This can be achieved by strengthening and growing law enforcement training and capacity building programs that equip Federal law enforcement, and our partners, with the technical skills and tools necessary pursue the most sophisticated transnational criminals. Programs such as the Secret Service's National Computer Forensics Institute (NCFI), which yearly trains over 3,000 U.S. state and local law enforcement officials in computer investigations techniques, and the Department of State's International Law Enforcement Academies (ILEA), which provide instruction to foreign law enforcement partners on approaches to combatting cybercrime and illicit finance, are prime examples of initiatives that enhance these requisite capabilities.

Conclusion

Digital money is clearly of great interest to governments, businesses, and U.S. citizens, as demonstrated by the substantial research conducted and investments places into these assets. The Secret Service is focused on doing our part to address the challenges posed by the increasing use of digital money in furtherance of illicit activity, from ransomware, to money laundering, to the financing of violent extremists and terrorists. But we and our law enforcement partners, both domestic and foreign, must and can do more. We must dramatically expand our efforts, and continue to adapt our investigative tools and techniques, if we hope to stem the tide.

Chairwoman Slotkin, Ranking Member Pfluger, and members of this Subcommittee, I will conclude by reiterating what many of my predecessors have emphasized here before in this body: Those that seek to further their illicit activities through use of digital currencies, or the Internet more broadly, should have no illusions that they are beyond the reach of the law. Even those assets and services that purport to be "anonymous" can be tracked and interdicted. As the investigative work of the Secret Service and our law enforcement partners has over the years demonstrated: We are relentless in enforcing the law and will not

[21] *See*, The Cyberspace Solarium Commission Report, available at, https://www.solarium.gov/report.

stop until those who seek to harm the United States and its citizens are arrested, convicted, and punished to the fullest extent of the law.

Thank you again for the opportunity to appear before you today, and your continued support for the mission of the U.S. Secret Service. I look forward to working closely with this Committee, and with other Members of Congress, on our shared priorities. I look forward to answering your questions.