M E M O R A N D U M

To: Members of the Committee on Financial Services

From: Digital Assets, Financial Technology, and Inclusion Subcommittee Staff

Date: February 12, 2024

Subject: Subcommittee on Digital Assets, Financial Technology, and Inclusion Hearing: "Crypto Crime in Context Part II"

On Thursday, February 15, 2024, at 2:00 p.m. the Subcommittee on Digital Assets, Financial Technology, and Inclusion will hold a hearing entitled: "Crypto Crime in Context Part II: Examining Approaches to Combat Illicit Activity." The following witnesses will testify:

- **Caroline Hill**, Senior Director of Global Policy and Regulatory Strategy at Circle
- **Michael Mosier**, Co-Founder and Partner, Arktouros
- **Grant Rabenn**, Director, Financial Crimes Legal, Coinbase
- **Ari Redbord**, Global Head of Policy and Government Affairs, TRM Labs
- **Carole Noelle House**, Senior Fellow, Atlantic Council; Executive in Residence, Terranet Ventures

Overview of the Illicit Finance Landscape in Digital Assets

Recent Developments

According to the Department of Treasury (Treasury)'s 2024 National Money Laundering Risk Assessment, "the use of virtual assets for money laundering remains far below that of fiat currency and more traditional methods."[1] Treasury reported increased instances of bad actors seeking to use digital wallets, mixers, digital asset trading platforms, and other methods to transact and obfuscate the digital asset transactions.[2] However, Treasury concluded that "the use of anonymity-enhancing technologies and techniques for financial transactions by terrorist groups has been limited so far."[3]

Considerable focus has been placed on terrorists' use of digital assets to fund their operations. However, the evidence suggests it still pales in comparison to the use of traditional financial assets by terrorists. Indeed, Treasury's 2022 National Terrorist Financing Risk Assessment

[1] U.S. Department of the Treasury, "2024 National Money Laundering Risk Assessment," (Feb. 2024), https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf, pg. 59.
[2] *Id.*
[3] Supra note 1, at 22.

concluded that "the vast majority of terrorist funds raised in the United States still move through banks and money transmitters or are in cash."[4]

In addition to terrorists' use of digital assets, there has been considerable attention on the connection between digital assets and fraud, including pig butchering and ransomware.[5] Currently, the most common ransomware-related payment method in reported transactions is bitcoin.[6]

However, FinCEN reports that criminals are migrating towards advanced obfuscation methods to counter the traceability of these payments flows. FinCEN has also concluded that "threat actors [are] increasingly requesting payments in anonymity-enhanced cryptocurrencies (AECs) and avoiding reusing wallet addresses, chain hopping, and cashing out at centralized exchanges, and using mixing services and decentralized exchanges to convert proceeds."[7]

AML/CFT Considerations in Digital Assets

Currently, centralized exchanges, stablecoin issuers, and other entities are subject to BSA obligations. As MSBs, exchanges, issuers and entities are required to register with FinCEN; develop, implement, and maintain an effective AML program; file suspicious activity reports (SARs) and currency transaction reports (CTRs); appoint a chief compliance officer; conduct training; and maintain certain records.[8] In addition, entities are responsible for monitoring their platforms and blocking any users that are on OFAC's Sanctioned Designated National List or from a sanctioned jurisdiction.

Blockchain Analytics

Blockchain analytics companies, in partnership with law enforcement, have developed extensive capabilities analyzing transaction data. These companies can establish attribution between a public address visible on the blockchain and the individual that initiated the transaction. The plethora of information gleaned through these investigations has resulted in several large-scale discoveries of illicit activity in the digital asset ecosystem.[9] These discoveries would have been impossible had these criminals used traditional funding mechanisms. Importantly, the tracing capabilities of these blockchain analytics firms are developing almost as fast as the

---

[4] U.S. Department of the Treasury, "2022 National Terrorist Financing Risk Assessment," (Feb. 2022), https://home.treasury.gov/system/files/136/2022-National-Terrorist-Financing-Risk-Assessment.pdf, pg. 22.
[5] Supra note 1 at 6. According to Treasury's 2024 National Money Laundering Risk Assessment, "investment fraud involving virtual assets has rapidly increased in both the number of victims and losses, rising 183 percent between 2021 and 2022."
[6] FinCEN, "Financial Trend Analysis," (Nov. 1, 2022), https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20AnalysisRansomeware%20508%20FINAL.pdf, pg. 2.
[7] *Id.*
[8] Bank Secrecy Act, 31 U.S.C. §§ 5311-5336 (2023)
[9] Department of Justice, "South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin," (Oct. 16, 2019), https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child; Alexander Mallin and Luke Barr, "DOJ Seizes Millions in Ransom Paid by Colonial Pipeline," ABC News (Jun. 7, 2021), https://abcnews.go.com/Politics/doj-seizes-millions-ransom-paid-colonial-pipeline/.

technology itself. One analytics firm has developed a tool for law enforcement to use when criminals use AECs.[10] Others have built out tracing and surveillance capabilities around mixers.[11]

Current Authorities of U.S. Law Enforcement

FinCEN

FinCEN's mission is to safeguard the financial system through the collection, analysis, and dissemination of financial intelligence to law enforcement. FinCEN's Director is appointed by the Secretary of the Treasury and reports to the Under Secretary of the Treasury for Terrorism and Financial Intelligence. FinCEN exercises regulatory functions primarily under the Currency and Financial Transactions Reporting Act,[12] as amended by Title III of the USA PATRIOT Act,[13] and the Bank Secrecy Act (BSA). The BSA is the United States' first and most comprehensive federal AML/CFT statute. It authorizes the Secretary of the Treasury to issue regulations requiring banks and other financial institutions to establish AML programs and to file reports on financial activity that may have relevance for criminal, tax, and regulatory investigations or for intelligence or counterterrorism.

OFAC

The International Emergency Economic Powers Act (IEEPA), enacted by Congress in 1977, authorizes the President to impose economic sanctions on countries, groups, entities, and individuals in response to any unusual or extraordinary threat to the national security, foreign policy, or economy of the United States when the President declares a national emergency with respect to that threat.[14] OFAC administers and enforces economic and trade sanctions programs established by executive orders issued pursuant to IEEPA. These sanctions are primarily issued against countries and groups of individuals, such as terrorists and narcotics traffickers, who are involved in activities related to threats to the national security of the United States.

Gaps in Law Enforcement Authorities and Capabilities

Treasury's 2022 National Money Laundering Risk Assessment emphasized that "uneven and often inadequate regulation and supervision internationally allow virtual asset service providers (VASPs) and illicit cyber actors to engage in regulatory arbitrage and expose the U.S. financial

[10] Andrew Hayward, "U.S. Homeland Security Can Now Track Privacy Crypto Monero," Decrypt (Aug. 31, 2020), https://decrypt.co/40284/us-homeland-security-can-now-track-privacy-crypto-monero .
[11] See Chainalysis Twitter Feed: https://twitter.com/chainalysis/status/1496087885061181443
[12] 31 U.S.C. 5311 *et seq.*
[13] P.L. 107-56.
[14] The International Emergency Economic Powers Act (IEEPA), Pub. L. 95-223, 91 Stat. 1626 (1977), codified at 50 U.S.C. § 1701 et seq.

system to risk from jurisdictions where regulatory standards and enforcement are less robust."[15] Treasury's 2024 National Money Laundering Risk Assessment further reiterated this concern as it highlighted inconsistent implementation of international AML/CFT standards as a gap in law enforcements' reach and authorities.[16]

Actions Taken by Law Enforcement Against Illicit Actors

FinCEN

FinCEN has brought several enforcement actions against digital asset firms. In January 2023, FinCEN issued an order identifying Russian digital asset exchange, Bitzlato, as a "primary money laundering concern" under section 9714 of the Combatting Russian Money Laundering Act.[17] On October 19, 2023, FinCEN issued a notice of proposed rulemaking that would require domestic financial institutions and domestic financial agencies to implement certain recordkeeping and reporting requirements relating to transactions involving digital asset mixers.[18]

OFAC

OFAC has taken numerous actions against sanctions evaders who use the digital asset ecosystem.[19] Since November 28, 2018, OFAC has included many digital wallet addresses and even entire digital asset services in its designations. For example, OFAC has sanctioned three virtual currency exchanges, Suex, Chatex, and Garantex, as well as the largest darknet market in the world, Russia-based Hydra.[20] OFAC has also taken steps to counteract one of North Korea's cybercrime groups, the Lazarus Group, including sanctioning two digital asset mixers, Blender.io and Tornado Cash, that were used by North Korea to process their ill-gotten gains as well as

---

[15] U.S. Department of the Treasury, "National Money Laundering Risk Assessment," (Feb. 2022), https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf, pg. 41.
[16] U.S Department of the Treasury, "2024 National Money Laundering Risk Assessment," (Feb. 2024), https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf, pg. 62.
[17] FinCEN, "FinCEN Identifies Virtual Currency Exchange Bitzlato as a "Primary Money Laundering Concern" in Connection with Russian Illicit Finance," (Jan. 18, 2023), https://www.fincen.gov/news/news-releases/fincen-identifies-virtual-currency-exchange-bitzlato-primary-money-laundering.
[18] FinCEN, "Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern," (Oct. 23, 2023), https://www.federalregister.gov/documents/2023/10/23/2023-23449/proposal-of-special-measure-regarding-convertible-virtual-currency-mixing-as-a-class-of-transactions?ref=tftc.io
[19] Chainalysis, "OFAC and Crypto Crime: Every OFAC Specially Designated National with Identified Cryptocurrency Addresses," (Aug. 10, 2023), https://www.chainalysis.com/blog/ofac-sanctions/.
[20] U.S. Department of the Treasury, "Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex," (Apr. 5, 2022), https://home.treasury.gov/news/press-releases/jy0701; U.S. Department of the Treasury, "Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange," (Nov. 8, 2021), https://home.treasury.gov/news/press-releases/jy0471; U.S. Department of the Treasury, "Treasury Takes Robust Actions to Counter Ransomware," (Sep. 21, 2023), https://home.treasury.gov/news/press-releases/jy0364.

Chinese nationals that helped North Korea launder funds following attacks on several digital asset exchanges.[21]

Department of Justice (DOJ)

The Department of Justice both issues enforcement actions against criminals operating in the digital asset ecosystem as well as conducts seizures of illegally obtained digital assets. Most notably, on November 21, 2023, the DOJ announced that it had reached a settlement with the world's largest digital asset exchange, Binance.com, and its founder and chief executive officer, Changpeng Zhao for violations related to the BSA, failure to register as a money transmitting business, and IEEPA.

Legislative Proposals

H.R. 7156 - Combating Money Laundering in Cyber Crime Act

H.R. 7156 clarifies the U.S. Secret Service's (USSS) investigative authority over crimes related to illicit digital asset transactions. The Combating Money Laundering in Cyber Crime would grant the USSS authority to go after institutions that facilitate illicit finance with digital assets.

H.R._____ - To establish an Office of Innovation within the Financial Crimes Enforcement Network

This discussion draft codifies the "Office of Innovation" within FinCEN and assigns the FinCEN Innovation Officer to head this office. The office would have two main functions: 1) hosting "Innovation Hours" where participants, such as financial technology companies and regulatory technology companies, can discuss their innovations related to AML/CFT, and 2) support pilot programs that test innovative methods, processes, and technologies that may help financial institutions comply with AML/CFT regulations.

H.R. _____ - To require the Securities and Exchange Commission, Commodity Futures Trading Commission, and the Secretary of the Treasury to jointly carry out a study on decentralized finance

This discussion draft would require the Secretary of Treasury, in coordination with the SEC and CFTC, to issue a report on decentralized finance as well as require a separate report by the GAO, to be submitted within 1 year to the relevant committees. This discussion draft is similar to provision in the Financial Innovation and Technology for the 21st Century Act, which passed out of committee in July 2023.

H.R. ____ - *To require the Secretary of the Treasury to report on privacy-preserving technologies*

---

[21] U.S. Department of the Treasury, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash," (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916; U.S. Department of the Treasury, "U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats," (May 6, 2022), https://home.treasury.gov/news/press-releases/jy0768; U.S. Department of the Treasury, "Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group," (Mar. 2, 2020), https://home.treasury.gov/news/press-releases/sm924.

This discussion draft would require the Secretary of Treasury to submit a report, within one year, that examines the use of privacy-preserving technologies for digital assets. The report would also provide an overview of how other jurisdictions are mitigating illicit finance related to privacy-preserving technologies.

H.R. _____ - *To establish an information-sharing pilot program to combat the illicit use of digital assets*

This discussion draft establishes a pilot program between FinCEN, the Department of Justice, the Department of Homeland Security, the IRS, and the private sector to voluntarily share information related to illicit activity stemming from the use of digital assets. This pilot program would allow secure sharing of information between the government agencies and private sector entities about potential illicit activity involving digital assets. This pilot program would expire after five years.