CATO INSTITUTE | CENTER FOR MONETARY AND FINANCIAL ALTERNATIVES

November 1, 2022

Scott Rembrandt
Deputy Assistant Secretary
Office of Terrorist Financing and Financial Crimes
U.S. Department of the Treasury

Re: Ensuring Responsible Development of Digital Assets
Docket ID: 2022-20279

To Whom It May Concern:

We appreciate the opportunity to provide input to assist the U.S. Department of the Treasury (Treasury) in its effort to better understand digital assets (commonly known as cryptocurrencies).[1] The Cato Institute is a public policy research organization dedicated to the principles of individual liberty, limited government, free markets, and peace, and the Center for Monetary and Financial Alternatives focuses on identifying, studying, and promoting alternatives to centralized, bureaucratic, and discretionary monetary and financial regulatory systems. The opinions we express here are our own.

The request for comment offered many interesting questions that will help inform the Treasury's responses to executive order 14067. However, our comments will only specifically address the following questions: A.2, A.4, B.1, B.2, B.7, B.8, C.2, D.2., D.3, D.4, D.6, D.7, and E.1.

****

A.2. How might future technological innovations in digital assets present new illicit finance risks or mitigate illicit finance risks?

As the future of technological innovation continues to evolve, it's likely that new methods for both conducting and catching illicit activity will emerge. If the Treasury is interested in keeping pace with these innovations, it should study the private sector's efforts to combat illicit activity. Rather than expand—or even continue—the surveillance under the Bank Secrecy Act (as the Treasury suggested in response to executive order 14067),[2] the Treasury should instead look to how private

[1] U.S. Department of the Treasury, "Ensuring Responsible Development of Digital Assets; Request for Comment," Federal Register, September 20, 2022, https://www.federalregister.gov/documents/2022/09/20/2022-20279/ensuring-responsible-development-of-digital-assets-request-for-comment.
[2] Nicholas Anthony, "The Biden-Cryptocurrency Reports: Part 1, Action Plan to Address Illicit Financing Risks of Digital Assets," Cato Institute, September 19, 2022, https://www.cato.org/blog/biden-cryptocurrency-reports-part-1-action-plan-address-illicit-financing-risks-digital-assets; White House, "Executive Order on Ensuring Responsible Development of Digital Assets," Presidential Actions, March 9, 2022, https://www.whitehouse.gov/briefing-

actors are already regulating the cryptocurrency market. In doing so, sledgehammer policies like sanctions and other sweeping decrees should be set aside. Instead, the Treasury should focus on crafting targeted approaches that seek to directly mitigate issues to the extent that laws are clearly broken. Innocent Americans should not have to bear the cost of broad enforcement activities when targeted alternatives are widely, and readily, available.

For example, in contrast to the sweeping approach that comes with sanctions (e.g., the sanctions on Tornado Cash),[3] the private sector has taken a more refined approach by targeting individual bad actors.[4] Companies, organizations, and individuals have worked to publicly identify and remove bad actors from the market. A few freely available efforts include:

- Blockchain Detectives
    - Twitter accounts like "@ZachXBT" have become known as blockchain detectives, or "on-chain sleuths," seeking to independently research and raise awareness about potential fraud.[5] Likewise, some companies (i.e., Peckshield) have set up Twitter accounts to publish potential scam and phishing website alerts.[6]
- Blockchain Explorers
    - Etherscan, Blockchain.com, Blockchair, Blockstream, Blockcypher, and countless other websites make blockchains accessible for anyone.[7] Users can search for transactions, view wallets, explore blocks, and more with little to no prior knowledge of blockchain analytics.
- Alert Systems
    - Before interacting with someone on the Ethereum blockchain, a user can search the person's wallet address on Etherscan and find out through ETHPROTECT if their wallet is known to be associated with scams, hacks, or fraud.[8] Likewise, Chainabuse provides a platform for cryptocurrency users to file and read reports of potential scams.[9] Lastly, the Chainalysis and TRM Labs offer screening tools so cryptocurrency platforms may preemptively block anyone already sanctioned.[10]

---

room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/; For background information on the Bank Secrecy Act, see Norbert J. Michel and Jennifer J. Schulp, "Revising the Bank Secrecy Act to Protect Privacy and Deter Criminals," Policy Analysis No. 932, Cato Institute, July 26, 2022, https://www.cato.org/policy-analysis/revising-bank-secrecyact-protect-privacy-deter-criminals.

[3] Nicholas Anthony, "Treasury's Tornado Warning," Cato Institute, August 9, 2022, https://www.cato.org/blog/treasurys-tornado-warning.

[4] Nicholas Anthony and Ivane Nachkebia, "How the Market, Not Government, Regulates Cryptocurrency Crimes," Cato Institute, August 23, 2022, https://www.cato.org/blog/how-market-not-government-regulates-cryptocurrency-crimes.

[5] "ZachXBT," https://twitter.com/zachxbt.

[6] "PeckShieldAlert," https://twitter.com/PeckShieldAlert.

[7] See https://etherscan.io/; https://www.blockchain.com/; https://blockchair.com/; https://blockstream.info/; and https://live.blockcypher.com/.

[8] Samuel Haig, "Etherscan Launches Fraud Monitoring and Address Blacklisting," Coin Telegraph, April 15, 2020, https://cointelegraph.com/news/etherscan-launches-fraud-monitoring-and-address-blacklisting.

[9] See https://www.chainabuse.com/browse.

[10] Chainalysis, "Chainalysis Oracle for Sanctions Screening," https://go.chainalysis.com/chainalysis-oracle-docs.html; TRM Labs, "Prevent Sanctioned Crypto Addresses From Engaging with Your Platform," https://www.trmlabs.com/products/sanctions.

- Major Platforms' Efforts in Fighting Scams
    - Coinbase, Binance, Kraken, and others have launched initiatives to educate consumers on how to identify and avoid bad actors.[11]
- Uniswap Token Lists
    - In response to the exponential growth in the issuance of ERC-20 tokens on the Ethereum blockchain, Uniswap created "Token Lists"—a community-led initiative that helps users identify legitimate projects.[12]

Likewise, there are also paid services that seek to regulate the market:

- Specialized Audit and Blockchain Analysis Firms
    - Chainalysis, TRM Labs, Ciphertrace, Peckshield, Elliptic, Haechi Labs, and others all offer services for both the private and public sector in terms of auditing and analyzing blockchains.[13]

The examples listed above work with the unique nature of cryptocurrencies and blockchain technology, not against them. And unlike when sanctions were used in the case of Tornado Cash to seemingly ban code or when Operation Chokepoint was used to choke people off from the financial system entirely,[14] the examples listed above are cases where individual criminals were targeted, not entire systems. Finally, it's through targeted approaches that agencies that have partnered with these efforts have managed to go after the individual criminals.[15]

In closing, there's one more point that should be kept in mind: namely, the optimal amount of illicit activity is not zero.[16] As the Treasury moves forward, and consults other agencies on their efforts, it would be wise to consider the tradeoffs at hand. Ideally, the crime rate would be zero, but that is not a practical policy target for an ever-changing world. Increasing investigation and

---

[11] Coinbase, "Avoiding Cryptocurrency Scams," Help, https://help.coinbase.com/en/coinbase/privacy-andsecurity/avoiding-phishing-and-scams/avoiding-cryptocurrency-scams; Binance, "Caution on the Rising Number of Crypto Scams," FAQ, https://www.binance.com/en/support/faq/ba0e3b7e0e19495cbe690544ddaa9010.
[12] See https://tokenlists.org/.
[13] See https://www.chainalysis.com/; https://www.trmlabs.com/; https://ciphertrace.com/; https://peckshield.com; https://www.elliptic.co/; and https://haechi.io/en/.
[14] Alan Zibel and Brent Kendall, "Probe Turns Up Heat on Banks," Wall Street Journal, August 7, 2013, https://www.wsj.com/articles/SB10001424127887323838204578654411043000772; Nicholas Anthony, "Treasury's Tornado Warning," Cato Institute, August 9, 2022, https://www.cato.org/blog/treasurys-tornado-warning.
[15] Robert Stevens, "How Chainalysis Helps Catch Cryptocurrency Criminals," Decrypt, September 7, 2020, https://decrypt.co/41127/how-chainalysis-helps-catch-cryptocurrency-criminals; Kristine Johnson and Michael Garcia, "Digital Currencies' Role in Facilitating Ransomware Attacks: A Brief Explainer," Third Way, May 3, 2021, https://www.thirdway.org/memo/digital-currencies-role-in-facilitating-ransomware-attacks-a-brief-explainer; Tuan Phan, "Did the FBI Hack Bitcoin? Deconstructing the Colonial Pipeline Ransom," ISACA Now Blog, July 1, 2021, https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/did-the-fbi-hack-bitcoin-deconstructing-the-colonial-pipeline-ransom; and Office of Public Affairs, "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," Press Release, Department of Justice, June 7, 2021, https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.
[16] J.P. Koning, "Here's Why We Tolerate Fake Check Scams," American Institute for Economic Research, January 2, 2021, https://www.aier.org/article/heres-why-we-tolerate-fake-check-scams/; Patrick McKenzie, "The Optimate Amount of Fraud is Non-Zero," Bits About Money, September 2, 2022, https://bam.kalzumeus.com/archive/optimal-amount-of-fraud/.

enforcement budgets, restricting the market with new laws and regulations, banning cryptocurrency entirely, or launching a surveillance regime so large that every individual is without escape will all pose different costs. And as it stands, none of these costs are justified given the present evidence.

Just as paper and electronic checks are not banned due to the existence of fake check scams,[17] the future financial system should also be designed such that the costs and benefits of surveillance and enforcement are kept in mind as the Treasury seeks to remove bad actors.

A.4. What are the illicit finance risks related to decentralized finance (DeFi) and peer-to-peer payment technologies?

The illicit finance risks related to non-custodial, peer-to-peer payment technologies (i.e., self-hosted wallets) are unlikely to pose substantial differences from the risks posed by the use of cash, or paper currency. However, we want to take this time to stress the importance of distinguishing between custodial and non-custodial services (i.e., the presence of a third party) when it comes to applying the law to suspected cases of illicit finance.

Although the current financial surveillance regime within the United States has been steadily expanding for decades,[18] the application of this regime does have a few limitations still in place to protect the rights of Americans. For instance, although the current regime holds that Americans do not have Fourth Amendment protections over their financial records held with banks or other financial institutions, the Fourth Amendment does protect financial activity conducted without a third-party intermediary.[19] Most notably, the Fourth Amendment does apply when two individuals transact in cash through a hand-to-hand exchange or transact in cryptocurrency through an exchange between self-hosted wallets.

To the extent that the Treasury wishes to investigate alleged crimes conducted with peer-to-peer payment technologies, it should therefore be certain of whether third parties are involved and to what extent they are involved. In fact, the Treasury should simply operate under the assumption that the Fourth Amendment does apply when conducting investigations.

[17] For additional context on why it is important to tolerate fake check scams despite their costs, see J.P. Koning, "Here's Why We Tolerate Fake Check Scams," American Institute for Economic Research, January 2, 2021, https://www.aier.org/article/heres-why-we-tolerate-fake-check-scams/.
[18] Norbert J. Michel and Jennifer J. Schulp, "Revising the Bank Secrecy Act to Protect Privacy and Deter Criminals," Policy Analysis No. 932, Cato Institute, July 26, 2022, https://www.cato.org/policy-analysis/revising-bank-secrecyact-protect-privacy-deter-criminals; Nicholas Anthony, "The Right to Financial Privacy: Crafting a Better Framework for Financial Privacy in the Digital Age," Cato Institute, Working Paper No. 69, October 14, 2022, https://www.cato.org/working-paper/crafting-better-framework-financial-privacy-digital-age.
[19] Nicholas Anthony, "Why Don't Americans Have Stronger Financial Privacy Rights?," Cato Institute, October 28, 2021, https://www.cato.org/blog/why-dont-americans-have-stronger-financial-privacy-rights.

B.1. What additional steps should the United States government take to more effectively deter, detect, and disrupt the misuse of digital assets and digital asset service providers by criminals?

For addition steps to effectively deter, detect, and disrupt the misuse of cryptocurrency, see the answer to question E.1 below.

B.2. Are there specific areas related to AML/CFT and sanctions obligations with respect to digital assets that require additional clarity?

Regarding how anti-money laundering (AML), combatting the financing of terrorism (CFT), and sanctions obligations can be clarified, the treatment of cryptocurrencies held in self-hosted wallets is something that deserves more attention. For example, in a recent report,[20] the Department of Justice (DOJ) appeared to be confused about guidance issued by the Financial Crimes Enforcement Network (FinCEN) regarding the application of rules for money transmitter businesses. Although the DOJ did not cite the guidance it referred to explicitly, it appears that the DOJ was referring to the guidance issued on May 9, 2019, where FinCEN wrote:

> [Self-hosted] wallets are software hosted on a person's computer, phone, or other device that allow the person to store and conduct transactions in [cryptocurrency]. [Self-hosted] wallets do not require an additional third party to conduct transactions. In so far as the person conducting a transaction through the [self-hosted] wallet is doing so to purchase goods or services on the user's own behalf, they are not a money transmitter.[21]

As it stands, the guidance offered by FinCEN is indeed clear that self-hosted wallets are not money transmitters. However, it's possible that the prevalence of third parties in the traditional financial system has confused the DOJ and others. With this example in mind, the Treasury should not only seek to deliver additional clarifications regarding the limits of other laws absent a third-party intermediary, but to also make sure that those clarifications are broadcasted widely in effort to reach a consensus of understanding among the different agencies.

Unfortunately, it's not just broader misunderstandings that undermine the clarity of AML/CFT and sanctions obligations. Individual sanctions should also be better explained to the public if the public is expected to be able to comply with the law. For example, the recent sanctions on Tornado Cash failed to explain how the American public was expected to comply with the

[20] U.S. Department of Justice, "The Role of Law Enforcement in Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets," The Report of the Attorney General, September 6, 2022, https://www.justice.gov/ag/page/file/1535236/download.
[21] FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," FinCEN Guidance, FIN-2019-G001, May 9, 2019, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

sanctioning of a software protocol.[22] Consider just a few of the questions the public had immediately following the announcement of the sanctions:[23]

1. How does the Treasury justify adding an automated, open-source software protocol to the sanctions list when the list has been traditionally used for sanctioning individuals and their property?
2. Does the Treasury believe that Tornado Cash is a centralized mixing service akin to Blender.io?
3. Does the Treasury believe that a single person or group ultimately controls Tornado Cash?
4. Does the Treasury believe the smart contracts within Tornado Cash can be changed at will by a single person?
5. How does the Treasury justify restricting open-source software when code is considered speech and protected under the First Amendment to the U.S. Constitution?
6. If a carbon copy were to be made of Tornado Cash (say, "Twister Cash" or "Typhoon Cash"), would using that iteration of the code be in violation of the sanctions on Tornado Cash?
7. Will the Treasury target specific iterations of code and thus lead the Specially Designated Nationals and Blocked Persons (SDN) List to become an ever-expanding list of specific open-source software protocols? Or does the Treasury plan to place blanket bans on entire forms of code?
8. If a person has complete control over his or her self-hosted wallet and receives funds through Tornado Cash, how does the person segregate the sanctioned funds? Should the sanctioned funds be sent to a new wallet for segregated storage? Should the person send the funds to the Treasury to be exchanged for non-sanctioned funds of equal or greater value in form the person requests?
9. If a person has sanctioned funds, should the funds received from the sanctioned source be segregated or is it sufficient to segregate some combination of those funds of equal value?
10. If a wallet holds a specific cryptocurrency and later receives a transaction of that cryptocurrency from a blocked address, are all the funds in that wallet considered "tainted"?

It was only weeks after the sanctions were announced that some questions were answered.[24] But even then, the questions addressed were neither addressed sufficiently in scope or in time. While barring all Americans from engaging with open-source software is objectionable in and of itself,

[22] Nicholas Anthony, "Treasury's Tornado Warning," Cato Institute, August 9, 2022, https://www.cato.org/blog/treasurys-tornado-warning.

[23] This sample of questions was collected from the following commenters. DeFi Education Fund, "Tornado Cash Update; EU Contemplates AML Regulator; Our Response to Treasury's RFC," August 22, 2022, https://www.defieducationfund.org/post/tornado-cash-update-eu-contemplates-aml-regulator-our-response-to-treasury-s-rfc; Jerry Brito and Peter Van Valkenburgh, "Analysis: What Is and What Is Not a Sanctionable Entity in the Tornado Cash Case," Coin Center, August 15, 2022, https://www.coincenter.org/analysis-what-is-and-what-is-not-a-sanctionable-entity-in-the-tornado-cash-case/; Drew Hinkes, Twitter Thread, August 17, 2022, https://twitter.com/propelforward/status/1560000600103854082?s=20&t=aQ8C41A_Zed_gWnbfJkUZw.

[24] DeFi Education Fund, "Tornado Cash FAQs; White House Crypto Climate Report; SEC's Newest Crypto Unit," September 15, 2022, https://www.defieducationfund.org/post/tornado-cash-faqs-white-house-crypto-climate-report-sec-s-newest-crypto-unit.

the Treasury should have at least supplied both its reasoning and its instructions to the public ahead of time.

B.7. What additional steps should the U.S. government consider to address the illicit finance risks related to mixers and other anonymity-enhancing technologies?

Before making decisions regarding anonymity-enhancing technologies, the U.S. government should take into consideration the fact that these technologies are neutral by nature. Like any other technological innovation, mixers and other anonymity-enhancing technologies can be used for both legal and illegal purposes. For example, Chainalysis found that less than 30% of the funds sent through Tornado Cash were connected to illicit actors.[25] Although the bad actors in question (i.e., the Lazarus Group) are indeed worthy of investigation, the broader public should not be punished for their crimes.

That so many people (i.e., the 70% of legal transactions sent through Tornado Cash) desire financial privacy should not be a surprise either. Access to privacy-enhancing technologies is extremely important in the cryptocurrency space. Unlike the activities in the traditional financial system, blockchain transactions are visible to the public. Anyone at any time is able to check the blockchain. But there are many examples where someone may not wish to have this data public. Whether it be a donation to a political campaign, religious institution, or maybe a cheat day on a diet, there are plenty of reasons for everyday citizens to desire financial privacy. And this reality is something even the Supreme Court has recognized.[26]

Moreover, tools like Tornado Cash are critical for cryptocurrency users living in countries run by totalitarian governments. For example, the co-founder of Ethereum, Vitalik Buterin, famously claimed he used Tornado Cash to donate to Ukraine amidst the Russian invasion in early 2022.[27] According to Buterin, he used the tool to protect not himself but the recipients of the donation.[28] While only a single anecdote, this story makes it clear how mixers and other privacy-enhancing technologies can be vital in helping oppressed communities around the world.

Fortunately, the necessary tools to fight individual criminals, and avoid using radical measures like banning decentralized software protocols, are available. First, when considering the illicit finance risks related to mixers and other anonymity-enhancing technologies, the U.S. government should seek to answer two initial questions:

[25] Chainalysis, "Understanding Tornado Cash, Its Sanctions Implications, and Key Compliance Questions," Chainalysis Blog, August 30, 2022, https://blog.chainalysis.com/reports/tornado-cash-sanctions-challenges/.
[26] California Bankers Association, 416 U.S. at 93–95.
[27] See https://twitter.com/VitalikButerin/status/1556925602233569280?s=20&t=YNrKsPWV_BaKC4VRunIj_Q.
[28] See https://twitter.com/VitalikButerin/status/1556978967554433024?s=20&t=s96zCIbvoBfHcp2iacBjzg.

1. Is the target an individual using the software or the software itself?
    a. An individual? Proceed to the next question.
    b. The software? Code is protected under the First Amendment.[29] Stop and reevaluate the problem being faced.
2. Is the individual being targeted for committing a crime and covering it up or is the individual being targeted for using a privacy-enhancing technology?
    a. Committing a crime? Proceed by using blockchain analytics to investigate and prosecute the individual, not the entire system (See response to question A.2 above). As noted by Jonathan Levin, co-founder of Chainalysis, and Eun Young Choi, director of the National Cryptocurrency Enforcement Team at the Department of Justice, mixers do not make it impossible for law enforcement to follow the money.[30]
    b. Using privacy-enhancing technology? Stop and reevaluate the problem being faced.

A process as simple as this one could have avoided the issues that arose when Tornado Cash was sanctioned. And a process as simple as this one would be wise to incorporate into future efforts.

B.8. What steps should the U.S. government take to effectively mitigate the illicit finance risks related to DeFi?

For steps to effectively mitigate the illicit finance risks related to DeFi, see answers to questions A.2, A.4., B.1., and B.7 above.

C.2. Are there specific countries or jurisdictions where the U.S. government should focus its efforts, through bilateral outreach and technical assistance, to strengthen foreign AML/CFT regimes related to virtual asset service providers?

The U.S. government should not focus its efforts to strengthen foreign AML and CFT regimes related to cryptocurrencies or the broader financial market. Although it would be a heroic assumption to make, if one assumes the AML and CFT regime within the United States works perfectly, that does not mean it can be exported to other countries seamlessly or without consequence.

In fact, one need not look far to see examples of these risks. It was only earlier this year when the Canadian government weaponized its own financial system to freeze the bank accounts of protestors.[31] And this financial oppression is a regular event for authoritarian countries like

[29] Alison Dame-Boyle, "EFF at 25: Remembering the Case that Established Code as Speech," Electronic Frontier Foundation, April 16, 2015, https://www.eff.org/deeplinks/2015/04/remembering-case-established-code-speech.
[30] United States Senate Committee on Banking, Housing, and Urban Affairs, "Understanding the Role of Digital Assets in Illicit Finance," Full Committee Hearing, March 17, 2022, https://www.banking.senate.gov/hearings/understanding-the-role-of-digital-assets-in-illicit-finance; Chris Brummer, "October 11: The Future of Crypto and Blockchain," October 11, 2022, https://www.youtube.com/watch?v=Kzcb9cRlEpI.
[31] Norbert Michel and Nicholas Anthony, "Keep Your Coins, Canada," Cato Institute, February 15, 2022, https://www.cato.org/blog/keep-coins-canada; Nicholas Anthony, "How Canada Made the Case for Cryptocurrency,

Russia, China, and South Sudan.[32] The protections (limited as they may be) for the rights of Americans are far better than many other countries around the world. To ignore these differences is to risk only putting people around the world at risk of further oppression.

D.2. How can the U.S. Department of the Treasury, in concert with other government agencies, improve guidance and public-private communication on AML/CFT and sanctions obligations with regard to digital assets?

For ideas on how the Treasury, in concert with other government agencies, can improve guidance and communication on AML/CFT and sanctions obligations, see the response to question B.2 above.

D.3. How can Treasury encourage the use of collaborative analytics to address illicit financing risks associated with digital assets while also respecting due process and privacy?

With respect to due process and privacy, the Treasury should end, or greatly reduce, its practice of sweeping financial surveillance under the Bank Secrecy Act. Although it is ultimately the duty of Congress to repeal or amend the Bank Secrecy Act itself,[33] the Secretary of the Treasury was charged with deciding much of its implementation. For example, the details regarding the reporting of currency transaction reports (CTRs) were originally decided by the Treasury. Something as simple as updating the $10,000 threshold for CTR reporting for the inflation that has occurred over the last 50 years could greatly improve the Treasury's respect for due process and privacy (See Figure 1).

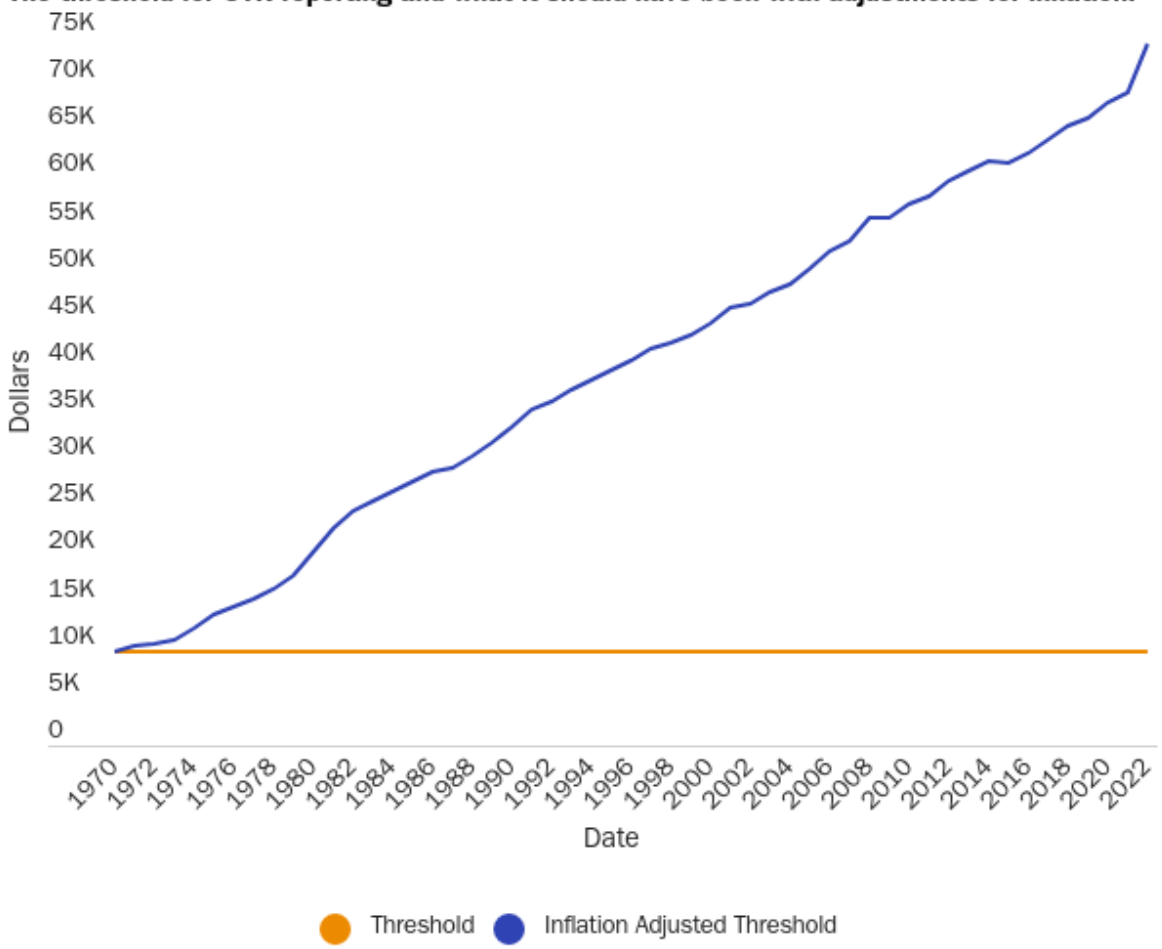
Not CBDCs," Cato Institute, March 2, 2022, https://www.cato.org/blog/how-canada-made-case-cryptocurrency-not-cbdcs.

[32] Andrew Osborn, "Russia Freezes Bank Accounts Linked to Opposition Politician Navalny," Reuters, August 8, 2019, https://www.reuters.com/article/us-russia-politics-navalny/russia-freezes-bank-accounts-linked-to-opposition-politician-navalny-idUSKCN1UY1ER; Sumeet Chatterjee and Clare Jim, "Hong Kong Bank Account Freezes Rekindle Asset Safety Fears," Reuters, December 8, 2020, https://www.reuters.com/article/hongkong-security-banks/hong-kong-bank-account-freezes-rekindle-asset-safety-fears-idUSKBN28I1ZK; Deng Machol, "South Sudan Order Bank Accounts of Activists Frozen," AP News, October 7, 2021, https://apnews.com/article/business-riek-machar-africa-south-sudan-e5cd55da29db3ef3740aacde133682df/.

[33] Norbert J. Michel and Jennifer J. Schulp, "Revising the Bank Secrecy Act to Protect Privacy and Deter Criminals," Policy Analysis No. 932, Cato Institute, July 26, 2022, https://www.cato.org/policy-analysis/revising-bank-secrecyact-protect-privacy-deter-criminals.

Figure 1

The threshold for CTR reporting and what it should have been with adjustments for inflation.



Source: Bureau of Labor Statistics

This hidden expansion of the Treasury's surveillance activities has been a 50-year-long encroachment of Americans' financial privacy with little to no checks and balances. Considering it was just a few years ago that FinCEN judged inflation as having been significant enough to warrant an increase for its monetary penalties, similar adjustments should be warranted to finally stop this 50-year-long encroachment on Americans' financial privacy.[34]

[34] Financial Crimes Enforcement Network, "Civil Monetary Penalty Adjustment and Table," Federal Register, June 30, 2016, https://www.federalregister.gov/documents/2016/06/30/2016-15653/civil-monetary-penalty-adjustment-and-table.

D.4. What technological solutions designed to improve AML/CFT and sanctions compliance are being used by the private sector for digital assets? Can these technologies be employed to better identify and disrupt illicit finance associated with digital assets and if so, how?

One example of a technological solution designed to improve sanctions compliance is the Chainalysis Sanctions Oracle.[35] In short, the oracle can be incorporated to check whether wallet addresses are on the SDN List in real time. Chainalysis and TRM Labs also provide a sanctions screening API so this feature can be incorporated in other areas.[36] Wallet addresses that have been listed are immediately blocked from transacting with the host. Chainalysis not only updates the oracle to reflect the lists from the United States, European Union, and United Nations, but it also allows anyone to use it free of charge.

While this offering, and others like it, is an impressive innovation within the market, it's important to note that this technology can only be employed to better disrupt illicit finance associated with cryptocurrencies if the Treasury is willing to let it. The developers of Tornado Cash had implemented this very procedure within the limited confines of the website they had control over.[37] However, the decision to sanction the software protocol effectively told the industry that such efforts were pointless. If the Treasury wishes to see technological solutions designed to improve compliance, it should explain when those efforts are deemed insufficient.

D.6. How can law enforcement and supervisory efforts related to countering illicit finance in digital assets better integrate private sector resources?

For steps for law enforcement and supervisory efforts related to countering illicit financial activity to better integrate private sector resources, see responses to questions A.2, A.4., B.1., and B.7 above.

D.7. How can Treasury maximize the development and use of emerging technologies like blockchain analytics, travel rule solutions, or blockchain native AML/CFT solutions, to strengthen AML/CFT compliance related to digital assets?

For steps to better maximize the use of blockchain analytics and other blockchain native solutions, see responses to questions A.2, A.4., B.1., and B.7 above.

[35] Chainalysis, "Chainalysis Oracle for Sanctions Screening," https://go.chainalysis.com/chainalysis-oracle-docs.html; TRM Labs, "Prevent Sanctioned Crypto Addresses From Engaging with Your Platform," https://www.trmlabs.com/products/sanctions.
[36] Chainalysis, "Free Sanction Screening Tools for The Cryptocurrency Industry," https://go.chainalysis.com/crypto-sanctions-screening.html.
[37] Macauley Peterson, "Tornado Cash Spins Up Sanctions-Compliant Web Interface," Blockworks, April 2022, https://blockworks.co/tornado-cash-spins-up-sanctions-compliant-web-interface/.

E.1. How can Treasury most effectively support the incorporation of AML/CFT controls into a potential U.S. CBDC design?

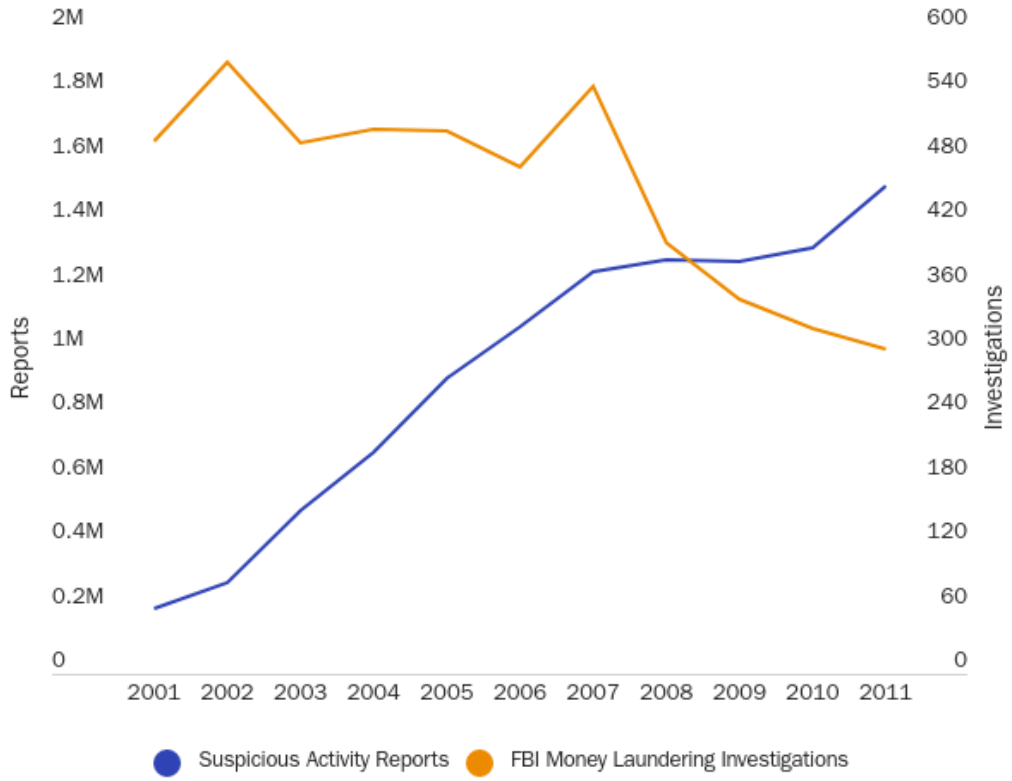
The U.S. government should reevaluate its entire approach to deterring, detecting, and disrupting the misuse of financial services before planning to incorporate AML and CFT controls into a potential U.S. CBDC.

The financial surveillance regime born out of the Bank Secrecy Act has involved ever-expanding surveillance with little evidence to justify the loss of privacy for Americans.[38] As Norbert Michel and David Burton found in 2016, money laundering investigations by the FBI had largely fallen despite the number of suspicious activity reports rising significantly (Figure 2).[39] In fact, the Bank Policy Institute appeared to confirm those findings when it found that only 3.58% of suspicious activity reports and 0.44% of currency transaction reports required a follow up from law enforcement (Figure 3).[40] Meanwhile, over 20 million reports had been filed as required by the current system—costing U.S. businesses an estimated $26.4 billion.[41]

[38] Nicholas Anthony, "How Inflation Erodes Financial Privacy," Cato Institute, June 10, 2022, https://www.cato.org/blog/how-inflation-erodes-financial-privacy.
[39] Norbert Michel and David Burton, "Financial Privacy in a Free Society," Heritage Foundation, 2016, https://www.heritage.org/markets-and-finance/report/financial-privacy-free-society.
[40] To be clear, this measure is only a proxy measurement for reporting effectiveness. Bank Policy Institute, "Getting to Effectiveness-Report on U.S. Financial Institution Resources Devoted to BSA/AML & Sanctions Compliance," October 29, 2018, https://bpi.com/getting-to-effectiveness-report-on-u-s-financial-institution-resources-devoted-to-bsa-aml-sanctions-compliance/.
[41] Financial Crimes Enforcement Network, "What is the BSA Data?," https://www.fincen.gov/what-bsa-data; LexisNexis, "True Cost of Financial Crime Compliance Study for the United States and Canada," 2022, https://risk.lexisnexis.com/insights-resources/research/2019-true-cost-of-aml-compliance-study-for-united-states-and-canada.

Figure 2

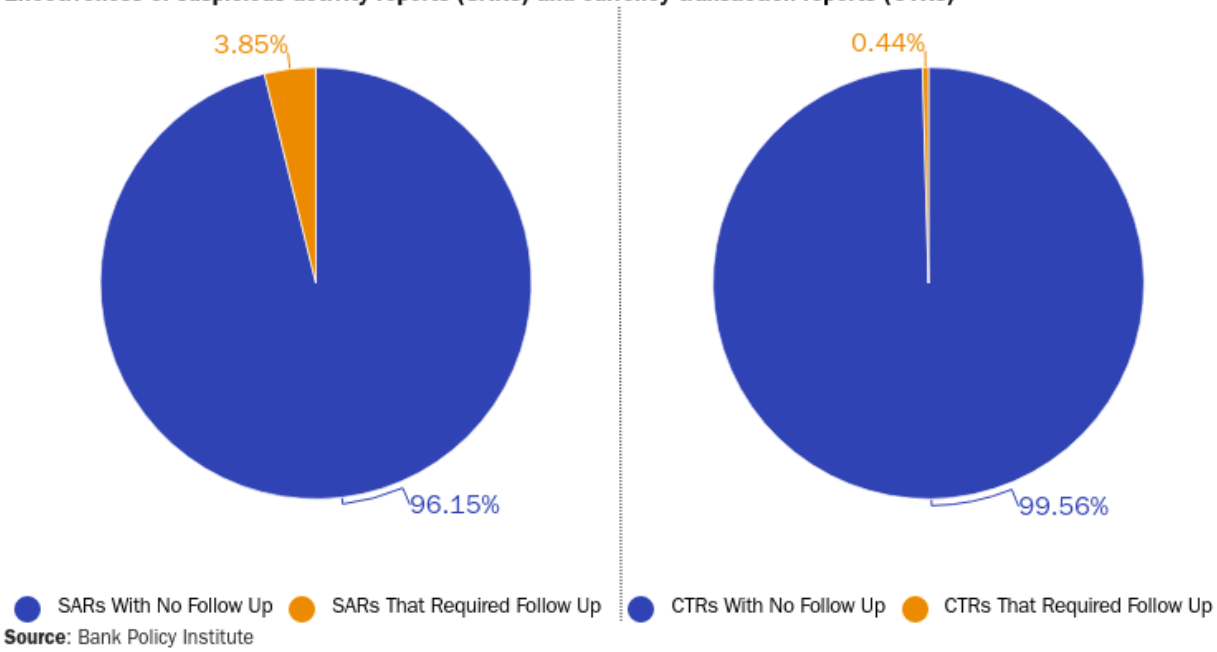
Suspicious activity reports versus FBI money laundering investigations



Source: Norbert Michel and David Burton, "Financial Privacy in a Free Society," Heritage Foundation, 2016, https://www.heritage.org/markets-and-finance/report/financial-privacy-free-society

Figure 3

Effectiveness of suspicious activity reports (SARs) and currency transaction reports (CTRs)



Source: Bank Policy Institute

Therefore, to best incorporate AML and CFT controls into the design of a potential U.S. CBDC (if Congress explicitly calls for the creation of a CBDC through passed legislation), the Treasury should first re-assess the costs and benefits of the current financial surveillance regime to identify where and to what extent the current regime should be cut down. To start, the Treasury should publicly publish a report with aggregate numbers (i.e., high-level statistics containing no personal identifying information) regarding the following:

- How many Bank Secrecy Act reports have been received by the Financial Crimes Enforcement Network;
- How many Bank Secrecy Act reports have been reviewed by the Financial Crimes Enforcement Network;
- How many Bank Secrecy Act reports have been requested by other governmental agencies;
- How many Bank Secrecy Act reports Act have led to a secondary investigation by the Financial Crimes Enforcement Network;
- How many Bank Secrecy Act reports have led to further procedures by law enforcement agencies including the use of a subpoena, warrant, or other legal process;
- How many Bank Secrecy Act reports have resulted in a conviction or settlement; and
- How many Bank Secrecy Act reports have resulted in additional charges in investigations unrelated to money laundering.

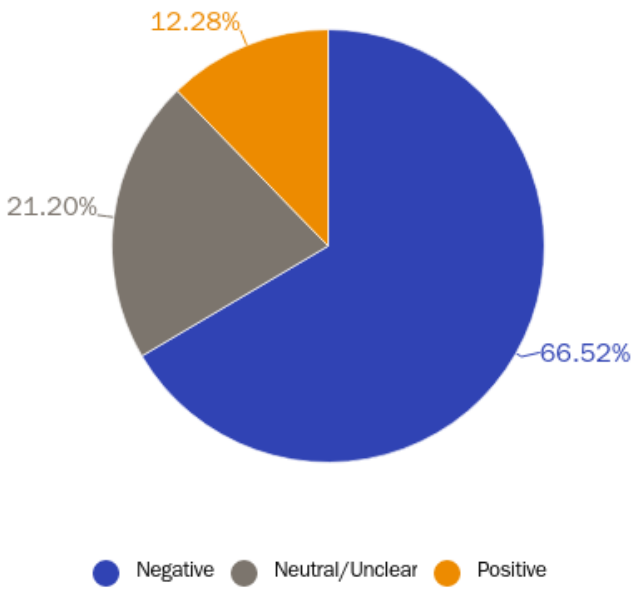
A public report detailing these statistics could raise awareness regarding the effectiveness and efficiency, or lack thereof, of the current financial surveillance regime. And it is this understanding that should be in mind before considering *how* to incorporate the legacy system into a potential CBDC.[42]

With that said, the Treasury should also be cautious regarding whether it will incorporate AML and CFT controls at all into the design of a potential U.S. CBDC. When the Federal Reserve published its discussion paper on CBDCs, it requested public feedback. Over two thousand responses were received and of them, over two thirds of the responses were concerned or outright against the prospect of a potential U.S. CBDC due to the risks to financial privacy, financial freedom, and the stability of banking system (Figure 4).[43]

[42] As famously noted by fictional chaos theorist, Ian Malcolm, it is important to not be so preoccupied with what could be done that no one stops to ask what should be done. Steven Spielberg, "Jurassic Park," Universal Pictures, 1993.
[43] Nicholas Anthony, "Update: Two Thirds of Commenters Concerned about CBDC," Cato Institute, July 27, 2022, https://www.cato.org/blog/update-two-thirds-commenters-concerned-about-cbdc.

Figure 4

Sentiment regarding the potential launch of a central bank digital currency (CBDC) in the United States.



Source: Author's calculations based on the responses to the Federal Reserve's request for comment on its CBDC discussion paper.

Turning a CBDC into a surveillance tool would not only make it unlikely that Americans will wish to use it, but also it would likely spark upset across the country akin to when the Treasury previously proposed monitoring bank accounts at least $600 of annual activity.[44]

****

Thank you for the opportunity to provide input to assist the Treasury in its effort to better understand cryptocurrencies.

Sincerely,

Nicholas Anthony
Policy Analyst
Center for Monetary and Financial Alternatives
Cato Institute

Ivane Nachkebia
DeFi Fellow
Center for Monetary and Financial Alternatives
Cato Institute

[44] Department of the Treasury, "General Explanations of the Administration's Fiscal Year 2022 Revenue Proposals," May 2021, https://home.treasury.gov/system/files/131/GeneralExplanations-FY2022.pdf.