TESTIMONY OF

Michael Mosier

BEFORE THE

U.S. House Financial Services Committee, Subcommittee on Digital Assets, Financial Technology and Inclusion

"*Crypto Crime in Context Part II: Examining Approaches to Combat Illicit Activity*."

February 15, 2024

Introduction

Thank you for allowing me to speak on topics to which I have dedicated nearly all my career: countering exploitation and supporting the democratization of opportunity.

My views are informed by experience as Acting Director, Deputy Director and Digital Innovation Officer of the Financial Crimes Enforcement Network (FinCEN); Counselor for Cybersecurity & Emergent Technology to the current Deputy Secretary of the Treasury; Associate Director of the Office of Foreign Assets Control (OFAC), leading the Office of Enforcement & Compliance and Office of Sanctions Policy & Implementation; Director for transnational organized crime at the White House National Security Council; a Deputy Chief in the Money Laundering Section at the U.S. Department of Justice (DOJ); chief technical counsel at Chainalysis blockchain analytics; and adjunct professor of advanced evidence for trial at Georgetown Law.

I come to this hearing only in my personal capacity. But informed by both my public and private sector experience, which includes, in addition to the above, co-founding a legal boutique[1] to represent whistleblowers, human rights activists, cryptographers, and developers across both civil society and emerging technology, broadly, and investing in agentic technology[2] that advances democratic resilience and personal agency, including deep-fake detection, cybersecurity and cryptography, as a partner an early stage venture fund,[3] without a narrow focus on digital assets in any of this. In my private sector work, I have dedicated myself to the same ideals as in my public sector work, enshrined in the mission of the Treasury Department: "*promoting economic prosperity and ensuring the financial security of the United States*."[4]

Supporting empowerment while countering exploitation have been consistently interwoven policy goals at DOJ and Treasury. When I was at DOJ working on some of the first cases for what became the Kleptocracy initiative, we didn't just prosecute corruption, we also worked to return assets to civil society groups in an overall effort to support democracy. When I was Associate Director at OFAC, we not only created sanctions programs to defend national security, we created exemptions for humanitarian aid as well as the free flow of information and censorship-resistant

[1] Arktouros pllc (https://www.arktouros.co/)
[2] https://buildexante.substack.com/p/agentic-tech-to-counter-digital-authoritarianism
[3] ex/ante (https://www.buildexante.com/)
[4] https://home.treasury.gov/about/general-information/role-of-the-treasury#

technology like VPNs to human rights activists under authoritarian regimes, as reflected in General Licenses D-1 and D-2 related to Iran.

When I was Deputy Director and Acting Director of FinCEN, we launched a privacy enhancing technology program and created a digital identity role in the Front Office, for proactive protection of personal data, to prevent victims, not just avenge them after the fact. We launched an innovation initiative and established a cryptocurrency senior role, to promote accessible, economic flourishing, consonant with Treasury's mission.

I promote these same ideals in the private sector and have been a proponent of appropriately managing risk in the emerging crypto space. I recently co-authored a 45-page research paper entitled "*Genuine DeFi as Critical Infrastructure: A Conceptual Framework for Combating Illicit Finance Activity in Decentralized Finance*,"[5] that proposed a framework for doing just this. It calls for effective ways to manage illicit finance risk, drawing directly upon existing, successful principles and practices involving financial-related critical infrastructure, since the software for crypto networks are fundamentally cyber infrastructure, not financial institutions. This proposal includes calling for *more* involvement, not less, of Treasury's Office of Cybersecurity & Critical Infrastructure Protection (OCCIP), with whom I had the opportunity to work directly, when I was Counselor for Cybersecurity & Emergent Technology to Treasury's Deputy Secretary Adeyemo.

The research and recommendations in the paper were based on knowing what works and has been working with respect to the critical technology and software underlying much of financial services today in the United States. Unfortunately, this workable framework is being ignored due to a newly developed obsession with treating every domino and marble of code in the Rube-Goldberg machine of financial networks as a bank itself that collects KYC on every data packet that is mathematically validated. I say "newly developed" obsession, because — for example — the Remote Procedure Call (RPC) communication technology that is part of the blockchain ecosystem has *actually* been part of network infrastructure — including the infrastructure underlying traditional financial services — since the 1970s, as a protocol to communicate between software programs across networks.[6] Never in the last fifty-plus years has there been a call for pure technological infrastructure providers to KYC each transported data packet. If they had, we would likely have a very different Internet today, if we would even have a truly global, neutral infrastructure at all. Russia-net and Iran-net likely would not connect to U.S.-net. However, neither would the pro-democracy political dissidents and human rights activists in those countries, reaching out for information and hopefully inspiration — a national security and foreign policy priority enshrined by Congress in the Berman Amendment.

[5] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4607332

[6] RPC is a widely used software communication protocol that one software program can use to request a service from another software program that is running on a separate computer or network. *See* John Barkley, U.S. Dep't of Com., NISTIR 5277, Comparing Remote Procedure Calls, (1993), https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir5277.pdf.

Treating every piece of financial-related mechanism as a "financial institution" overestimates the safety of "financial institutions" and effectiveness of KYC.

There is an unsupported presumption that newer, distributed technological infrastructure supporting financial operations should be treated very differently from the infrastructure underpinning traditional finance (TradFi) networks, because TradFi purportedly has trustworthy gatekeepers that keep us safe, much through the success of KYC. For a number of reasons, this presumption is leading us away from our experience with what actually works. **First**, we have to start with the recognition that blockchain is fundamentally code and cyber infrastructure, not "new banks." **Second**, I can say as a former prosecutor who obtained the first plea to hold a bank president responsible for violations of the BSA for having personally solicited Venezuelan black market peso operators — who were of course KYC'ed in — the current system still faces immense challenges in combating illicit financial activity. We have to question forcing software providers into KYC frameworks that both overemphasize identity over activity and are so fallible. **Third**, treating software underlying financial mechanisms as "critical infrastructure" has, for years, brought out significant and voluntary collaboration from not only financial institutions but also those who have no active involvement in the financial system except to build and host software that may be used as part of the system. Greater threat-information has been shared across relevant players to allow *all* to improve their resilience, because the opportunity to share through private-public coordination has not depended on everyone being a "financial institution," with all the accompanying burdens as well as false sense of security it projects.

The Bank Secrecy Act itself was named for the secrecy of Swiss and other banks that were a haven for U.S. mafia money launderers in the 1960's and 70s. Fast forward half a century and in 2021, FinCEN enforced against a major national bank for ongoing banking of a known, convicted mafia member. The bank had implemented KYC, but that did very little. The bank was fined $390 million for willful violations of the BSA. As FinCEN Director Kenneth Blanco said, "*[The bank] acknowledged…[it] had actual knowledge of criminal charges against specific customers, including Domenick Pucillo, a convicted associate of the Genovese organized crime family … [and] continued to process over 20,000 transactions valued at approximately $160 million, including cash withdrawals, for Pucillo's businesses*."[7]

The idea that banks are doing KYC and monitoring risks themselves, so any infrastructure around them is safer than financial mechanisms through traceable public blockchain systems is contrary to experience. Major banks doing KYC have paid ~$385 billion in penalties for fraudulent and illegal activity since 2000.[8] Further, the fiat wire infrastructure runs in anonymity-enhanced silos that make it virtually impossible for a U.S. prosecutor to trace transfers across banks in Russia, Iran, or North Korea (DPRK) — in contrast to public ledgers of blockchain — making KYC of limited use in global fiat flows. You can put hope-against-experience in a Mutual Legal Assistance Treaty (MLAT) request for information, *if* there even *is* a Legal Assistance Treaty with the country. But in the best-case scenario, that could easily take two to three years to get any of the information, and any request for the personally identifiable information of KYC will need to contend

[7] https://www.fincen.gov/news/news-releases/fincen-announces-390000000-enforcement-action-against-capital-one-national

[8] *See* https://violationtracker.goodjobsfirst.org/summary?major_industry_sum=financial+services.

with most EU governments' data protection laws. And if it is a bank in China, they will assert national security privilege over anything involving a bank, because they are state-owned, so there is little chance.

It is no surprise that Treasury itself has observed that TradFi illicit finance is exponentially greater than public ledger illicit activity, which is also far more knowable.[9] The original anonymity-enhanced technology is cross-border fiat banking with nested accounts and shell companies. JPMorgan Chase, for example, has paid more in criminal fines, settlements and violation charges[10] than has ever been laundered using bitcoin, and that is bitcoin on a transparent ledger where it is far more identifiable to law enforcement, compared to siloed bank branches with people trading ATM cards and online login credentials across drug cartels. In fact, the Sinaloa and Norte del Valle cartels laundered nearly $900 million in fiat currency through HSBC.[11]

KYC is failing people, through stolen credentials, virtual slavery, and deep-fakes.

Over-reliance on static, easily duped KYC and a false sense of security around it is creating greater risk. It has created a market for deep-fakes and stolen identities, which misdirects investigators to the wrong people, and is failing both the people we should be protecting and the public servants whose job it is to address illicit finance.

This is why at FinCEN, years ago, a vigilant member of the Intelligence Division rang the bell on the rapidly advancing capabilities and plummeting price of deep-fakes to undermine TradFi KYC processes. This led to our establishment of a Digital Identity position reporting directly to the Director. We saw this through the massive Paycheck Protection Program fraud, but even across everyday banking. Banks' reliance on KYC was becoming a misdirection, in an era of being able to buy identity data online in bulk for mere dollars and generate fake credentials with a few clicks of the mouse. KYC did not stop the laundering of hundreds of millions of dollars in violent cartel money into one of the largest banks in the world. Drivers licenses don't list the cartel or terrorist organization of which you're a member. "Neural networks" can now churn out fake IDs in minutes, bypassing KYC checks.[12] This is not to say there is no role for identity, just that we need to rethink identity-oriented risk, which is why we created the Digital ID position.

It is not just fake identities. KYC has generated a massive market for real, stolen or extorted identities from humans, both through theft and virtual slavery. There is reporting about a 26-year-old Thai single mother of three locked in a crowded compound, handing over phones and

[9] *"Still, as previously noted in the 2022 NRAs, this risk assessment recognizes that **most money laundering, terrorist financing, and proliferation financing by volume and value of transactions occurs in fiat currency or otherwise outside the virtual asset ecosystem via more traditional methods**."* U.S. Dep't of the Treas., Illicit Finance Risk Assessment of Decentralized Finance, p.4 (2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf (emphasis added).

[10] https://violationtracker.goodjobsfirst.org/parent/jpmorgan-chase

[11] https://www.justice.gov/opa/pr/hsbc-holdings-plc-and-hsbc-bank-usa-na-admit-anti-money-laundering-and-sanctions-violations

[12] https://www.404media.co/inside-the-underground-site-where-ai-neural-networks-churns-out-fake-ids-onlyfake/

passports to a Chinese-run investment scam.[13] There are reports of more than 2,700 workers from across SouthEast Asia trapped in virtual slavery and forced to participate in scams targeting people over the internet, fearing they would be sold to other syndicates.[14]

In the narco-trafficking world, we talk about the demand-side creating financial incentive for traffickers to produce, smuggle, and murder. KYC is creating this demand-side for identities, due to the siloed world of TradFi, where KYC is the passkey. This is less applicable in the on-chain world of immutable, traceable public ledgers, where activity-based risk monitoring is more accessible and harder to spoof than a fake ID. Public ledgers have led to the recovery of millions in hacked funds. Despite the Lazarus Group's off-ramping efforts, U.S. law enforcement has been able to follow the funds to cash-out points, freeze the assets and ultimately recover over $30 million.[15] The Norwegian government was able to recover another $6 million using similar methods.[16] These recoveries "*demonstrate that it is becoming more difficult for bad actors to successfully cash out their ill-gotten crypto gains*."[17]

KYC and supposedly trusted "financial institution" intermediaries are not the reason to treat software and technological infrastructure differently in TradFi than in public ledger technology. You are failing both the victims and the public servants in whose name you're invoking protection to reinforce moats that keep people from accessing more publicly transparent financial opportunity. There's a reason so many former law enforcement and national security officials support financial networks with resilient public ledgers that also help us get critical censorship-resistant support to human rights defenders in Iran and Venezuela.[18]

Activity-based, network analysis risk management in crypto.

This all points to the opportunity for alignment among policymakers and industry in reliable risk management for the cryptocurrency space. Activity-based risk is harder to spoof and readily detectable. Co-spending analysis of associated transactions between high-risk on-chain wallets can tell you that other wallets are likely part of high-risk activity and operators, just like law enforcement and analytics companies build out networks nearly instantaneously after one bad address is attributed either by OFAC or crowdsourced across the private sector from a hack. It doesn't wait for a photo, Social Security Number and middle name to freeze high-risk wallets while investigating the blockchain space. Violent cartels and terrorist organizations don't stamp passports used for KYC. You determine it through activity and associations with money movement. Network analysis, not drivers licenses.

[13] https://www.abc.net.au/news/2022-12-29/inside-call-centre-scams-in-cambodia-torture-fear-and-survival/101770352

[14] https://apnews.com/article/philippines-cybercrime-raids-china-indonesia-malaysia-vietnam-de16f11954700ffd432377267f571892

[15] Erin Plante, *$30 Million Seized: How the Cryptocurrency Community Is Making It Difficult for North Korean Hackers To Profit*, Chainalysis (Sept. 8, 2022), https://www.chainalysis.com/blog/axie-infinity-ronin-bridge-dprk-hack-seizure/.

[16] *Id*.

[17] *Id*.

[18] https://theblockchainassociation.org/wp-content/uploads/2024/02/NatSecLettertoCongress_2_13_24.pdf

While banks are checking paperwork on the various nested accounts and shell companies used to provide "KYC," for the full 30 days to file a SAR,[19] blockchain analytics are attributing risk to wallets in seconds, and companies like Circle are freezing stolen funds in minutes while investigations are pursued to confirm or correct. In the fiat world, once a wire crosses borders, your chances of getting anything back for victims diminishes precipitously. In the crypto world, the reach is global, fast, and far beyond what it takes to send one fiat wire and escape to a "protective" jurisdiction that will never give you the prized KYC, as the funds quickly skip to the next jurisdiction in the siloed, anonymity-enhanced world of fiat, from which the name of the Bank Secrecy Act itself comes.

Public Ledgers

In 2019, the Department of Justice announced the shutdown of Welcome to Video, one of the largest ever CSAM sites, and the arrest of the site's owner and operator.[20] Law enforcement arrested more than 337 site users across 38 countries (including UK, South Korea, Germany, Saudi Arabia, the UAE, the Czech Republic, Canada, Ireland, Spain, Brazil and Australia). Most importantly, at least 23 minors were identified and rescued from their abusers as a result of this investigation. The operation was made possible by tracking on-chain blockchain transactions, which allowed governments around the world to use analytics to quickly determine the location of the Welcome to Video's server and, ultimately, shut down its operation.

Because of the public ledger, law enforcement agents could access blockchain data and use analytics software to trace transactions, map out users of the site and disseminate the public blockchain evidence to their global partners without friction. They were able to view blockchain records regardless of where in the world they were created, without subpoenas, foreign courts, or agreements with foreign jurisdictions. They were able to share this information across 38 jurisdictions exponentially faster than private bank information, to rapidly take down the site and identify and rescue victims. The public ledger also showed which centralized exchanges had interacted with suspected wallets, so agents could go directly to the relevant exchanges and show them how the perpetrators interacted with their platform, to gather more information.

The Welcome to Video investigation demonstrates how public blockchain records can assist law enforcement to efficiently identify and trace bad activity. With fiat and opaque wire transfers that may involve shell companies and fake KYC across a web of non-compliant banks in high-risk jurisdictions with varying "bank secrecy" laws, we would spend months or years trying to estimate likely relevant, foreign banks for potential information on, using little more than guesses based on general understanding of regional banking players and correspondent relationships, then subpoenaing banks and using MLATs to try to transfer information between jurisdictions, which

[19] https://www.law.cornell.edu/cfr/text/12/21.11

[20] Press Release, U.S. Dep't of Just., South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin, (2019), https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child; For an additional case study on Welcome to Video, *see Chainalysis in Action: DOJ Announces Shutdown of Largest Child Pornography Website*, Chainalysis (Oct. 16, 2019), https://www.chainalysis.com/blog/chainalysis-doj-welcome-to-video-shutdown/.

takes years. With crypto, the public ledger shows immediately which centralized exchanges have interacted with suspected wallets, so you go directly to the relevant ones, and the conversation starts with showing them exactly how we know (with public data) that the suspected perpetrator interacted with their platform. The permanence of blockchain records also means that law enforcement officials can continue analyzing the data for years to come. As Chris Janczewski, one of the lead investigators in the case, stated "*If a bank was robbed five years ago and you're still trying to chase down those leads, you have no idea potentially where that stolen cash could be at this point. With cryptocurrencies, like bitcoin, every transaction is on a public ledger. It's public and is there forever*."[21]

Potential for Significant Alignment

At the same time, policymakers must not underestimate the significant advances of cryptographically secured and widely accessible networks that can enable their own democratic and financially inclusive policy goals, such as the Treasury Department-enabled humanitarian aid to 60,000 Venezuelan healthcare workers under an authoritarian government, which only succeeded because of the permissionless and non-intermediated nature of cryptocurrencies.[22]

The importance of cyber resilience for vulnerable populations, tied to foreign policy and national security goals, is longstanding. In 2002, OFAC updated it's well known General License D-1 to a new D-2, which Treasury Deputy Secretary Adeyemo described as "*helping the Iranian people be better equipped to counter the government's efforts to surveil and censor them*," reflecting "*the Administration's commitment to promoting the free flow of information*."[23] The press release notes that, "*While Iran's government is cutting off its people's access to the global internet, the United States is taking action to support the free flow of information and access to fact-based information to the Iranian people*."[24] The General License, in its own words, supports "*the communication tools to assist ordinary Iranians in resisting repressive internet censorship and surveillance tools deployed by the Iranian regime*" and "*protect the ability of Iranians to engage in free expression and bravely resist regime oppression*."[25] It also emphasizes that the General License "*expands existing case-by-case licensing policy, particularly to allow Iranian developers to create homegrown anti-surveillance and anti-censorship apps, which many Iranian people rely upon to circumvent domestic internet controls*."[26] There is great alignment between national security policy and censorship-resistant networks. This isn't just about financial integrity, it's about human dignity, and with cryptographically secure public ledgers, both are possible.

---

[21] Michelle Cho & Ken Dilanian, *Cryptocurrency May Not Be so Crime-Friendly after All. Federal Law Enforcement Is Getting Good at Tracing It*, NBC News (May 13, 2022), https://www.nbcnews.com/news/crime-courts/cryptocurrency-may-not-crime-friendly-federal-law-enforcement-getting-rcna23844.

[22] *Circle Partners with Bolivarian Republic of Venezuela and Airtm to Deliver Aid to Venezuelans Using USDC*, Circle (Nov. 20, 2020), https://www.circle.com/blog/circle-partners-with-bolivarian-republic-of-venezuela-and-airtm-to-deliver-aid-to-venezuelans-using-usdc.

[23] https://home.treasury.gov/news/press-releases/jy0974

[24] *Id.*

[25] *Id.*

[26] *Id.*

This sentiment has been reinforced by the current Director of National Intelligence, Avril Haines, who has said that rising digital authoritarianism poses "*a critical threat to our national security*," citing, in particular, the repressive models implemented by the Russian, Chinese and Iranian governments as efforts that undermine democratic values within their countries and beyond: "*[T]he use of these technologies and methods to monitor and limit dissent are on a trajectory to become even more pervasive, targeted and complex in the next few years, further constraining freedoms globally*."[27] Director Haines said that the rise of digital authoritarianism and surveillance tools to suppress internal dissent should activate the democratic nations to "*preserve, to the greatest extent, the promise of [emerging] technologies to support freer flows of information…while nevertheless guarding against their use for digital repression*."[28] These points from the Director of National Intelligence point to natural alignment with cryptographically secure, distributed networks as a matter of U.S. national security.

The methodology to manage risk will evolve just like moving from switchboard operators to mobile phones has changed how we do things. As with the development of web1 and 2, we did not just require internet companies to have a security guard at the door of their office and a listing in the Yellow Pages of the phone book so we can call them for problems. We developed internet-native risk management, like Cloudflare's DDOS protection to operate in real-time at the speed of the internet, not the speed of getting in your car and driving to the mall. Cybersecurity tools were developed that operate with far more agility on greater volume than any human reflex, automating risk detection for necessary speed and accuracy in addressing threats.

To be effective, we must recognize that blockchain networks are fundamentally cyber infrastructure, not "banks." Addressing cyber and code vulnerabilities will capture far more risks than a preoccupation with treating infrastructure as "financial institutions." KYC for a hacker only helps if the hacker has already been identified. But threat activity typologies may already be known, and/or evolve much faster than an OFAC or PEP list, to *prevent* victims, not just avenge them. We are better to capture the next Lazarus as a cyber threat well before it makes it all the way to a national emergency on the OFAC List. Ransomware (1989) predates crypto (2009) by two decades and was "enabled" by the internet and computers, not dependent on any one of the many payment methods used throughout time. The most impactful solutions to ransomware have been requirements by insurers that policyholders implement meaningful cybersecurity practices to reduce incidents from the beginning. Obsession with payments distracts from the real focus on better cybersecurity to prevent victims. Over-attributing cyberthreats to payments issues misses critical causes and preventive measures to be taken.

Recommendations

Certainly, there is work to be done yet for the next evolution of the financial networks to be safely accessible. The early internet had an uneven start as well. Instead of shutting it down or turning data routers into banks, we pursued pragmatic solutions rather than dogmatic categorization.

[27] https://www.nextgov.com/emerging-tech/2023/04/digital-authoritarianism-poses-critical-threat-national-security-intel-chief-says/385614/

[28] https://www.nextgov.com/emerging-tech/2023/04/digital-authoritarianism-poses-critical-threat-national-security-intel-chief-says/385614/

This kept the heart and mind of emerging global networks in the United States, anchored in democratic principles, and with information and expertise readily reachable.

Here are **two concrete actions** you could take to tangibly impact illicit finance:

1. First, **resource the existing FinCEN and OFAC authorities** before saying those aren't working. In the first Senate Banking hearing following the October 7 atrocities in Israel, I sat behind my former counterpart who was head of the Israeli FIU. Every witness in that hearing said two things consistently: (1) terrorist financing is overwhelmingly in fiat, not crypto; and (2) every authority needed to address these issues is "already in the President's hands," but the agencies are not resourced to carry them out.

   Throwing more shovels at people who already have 37 shovels in each hand doesn't make them more effective, it is setting them up for failure.

   Four years after the historic update and expansion of authorities by the AML Act of 2020, FinCEN and OFAC still have not received all of the roughly $74 million for resources, while more and more are demanded of them. Resource them for their current job, before burdening them – and industry – with more unfunded mandates. You gave them cars with no gas in them, and then are telling them they need new cars because they aren't getting anywhere with the old ones. Then a year ahead you'll bring them down to the Hill and demand numbers on miles they've driven with both the new and the old cars you gave them that had no gas. You had it right before, you just didn't deliver on what was authorized but not appropriated four years ago. Here is what remains un-funded:

   a. FinCEN's global **FIU Liaisons** have not been funded and deployed. The idea was fantastic, and leveraged impactful work on crypto illicit finance that we had already piloted under FinCEN's Egmont information sharing mechanism with other FIUs. We immediately mapped out the first placements to increase operational information-sharing beyond the generalized Treasury attachés doing economic diplomacy, four years ago. But we never got the promised funding.

   b. **FinCEN's Whistleblower Office** – Because we believed strongly in the vision, while awaiting funding, we took a position from another part of Enforcement to at least get someone to handle unofficial intake that was already happening. There are leads pouring into FinCEN, but Congress hasn't resourced it to succeed. Whistleblower offices are either a virtuous or vicious cycle: If people see leads followed, they take the time to send in more; if people don't see leads even responded to, they don't. Just last week there was an article in the WSJ about people complaining that there was not yet a dedicated whistleblower intake website for FinCEN. But as someone rightly observed, "*FinCEN's enforcement staff is only a fraction of [those at] agencies like the SEC and [CFTC], both of which have had great success [with whistleblower programs]. Congress could help greatly by appropriating more funds for the FinCEN program*." As the person noted, "*If I was to prioritize the issues, I would rank the relative lack of resources over the lack of a*

website."[29] The fact that these national security professionals are working against such great odds when Congress claims they need to help FinCEN by giving it more boats to row rather than any hands or oars for the current ones is not helping national security, it's setting them up for failure.

c. **Domestic Liaisons** - The AML Act set out positions for multiple Domestic Liaisons, including a Chief Domestic Liaison reporting to the Director. The concept was to situate liaisons in Federal Reserve territories across the country to engage around innovation and risk management expectations and effectiveness. Like the global FIU Liaisons, we immediately mapped out where they could be placed to optimize effectiveness, as we eagerly awaited the funding to be allowed to post for the positions and hire. You had a great idea. Please work with appropriators to get the authorized funds to FinCEN to do it.

d. **Innovation Officer** - The AML Act enshrined a version of the Digital Innovation Officer position I held, to drive both internal and external innovation. It is unfunded and unfilled.

e. **Chief Digital Currency Advisor** - Relatedly, we created and staffed a Front Office position of Chief Digital Currency Advisor, dedicated specifically to crypto issues.[30] That person left after I did, and the role has never been filled. The position was probably cannibalized for Beneficial Ownership work that also was not funded. However, given the number of hearings and press releases about the impending threat of crypto, it would seem reasonable to fund and fill the position at the U.S. FIU.

2. Second, capitalize on natural alignment around risk management and existing best practices by **treating cryptographic distributed networks as the cyber infrastructure it is** and **activating Treasury's Office of Cybersecurity & Critical Infrastructure Protection** (OCCIP) to coordinate information-sharing across the public and private sectors.

Given the natural alignment between counter-authoritarianism and cybersecurity in the crypto and national security spaces, a collaborative approach should be clearer than it is – particularly since exponentially greater illicit finance is happening through centralized actors in the fiat.[31] Cyber infrastructure that supports financial interactions is not new. Remote Procedure Call protocols have been around since the 1970s communicating between software programs across networks,[32] we just talk about them more prominently in web3. Likewise, data verification and transport has been underpinning digital commerce and online finance for decades. We know what works to secure infrastructure systems. But instead of focusing on shared interests to manage infrastructure risk, much of the policymaking world has been focused on expanding the

[29] https://www.wsj.com/articles/fincen-pressured-to-implement-anti-money-laundering-sanctions-whistleblower-program-84b2992f

[30] https://www.fincen.gov/news/news-releases/fincen-welcomes-first-ever-chief-digital-currency-advisor-and-first-director

[31] *"Still, as previously noted in the 2022 NRAs, this risk assessment recognizes that **most** money laundering, terrorist financing, and proliferation financing **by volume and value** of transactions occurs in **fiat** currency or **otherwise outside** the virtual asset ecosystem via more traditional methods."* U.S. Dep't of the Treas., Illicit Finance Risk Assessment of Decentralized Finance, p.4 (2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf

[32] *See* John Barkley, U.S. Dep't of Com., NISTIR 5277, Comparing Remote Procedure Calls, (1993), https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir5277.pdf.

definition of "banks" to make every data processor into a financial institution, collecting exceptionally sensitive KYC-related data sent to more people unqualified to protect it. This vastly increases our risk for compromised personal information, when we know that KYC can be so easily spoofed, and there are far more relevant activity-based risk indicators.

Instead, leverage the data accessibility of public ledgers and cryptographic systems to share threat typologies in the same way that OCCIP has been doing for years with financial infrastructure, without treating every recipient as a bank in order to do so. They might call AWS, Cisco or Comcast about an attack that could impact the financial system. It doesn't matter what the entity is, as long as it underpins financial networks. It doesn't mean those entities now need to collect everyone's Social Security Number whose data is transported on their networks; it means there is a shared interest in protecting infrastructure and a virtuous cycle in having the mechanisms to share information around threats and vulnerabilities. Yes, at times individuals need to be identified, but it is targeted and with a purpose, not data dumps into honey pots.

We lay much of this out in our 45-page paper on "*Genuine DeFi as Critical Infrastructure: A Conceptual Framework for Combating Illicit Finance Activity in Decentralized Finance*,"[33] so I will not elaborate here. But, in short, some elements of the crypto ecosystem are better placed to have helpful information and provide alerts than others, much of which can be real-time automated data reporting on threats like versions of DDOS attacks, spoofing, or code exploits. This is more cybersecurity because this is cyber infrastructure. Lazarus Group is on the OFAC List for its cyberthreats that also benefit DPRK, so being flagged among even more cyberthreats not yet on the OFAC list is good for everyone, in a very natural alignment. Obligations can be calibrated to where threats actually are happening, not every packet-switcher in the world, just like we already calibrate expectations across financial related infrastructure today, and some of it generates alerts in different ways that are optimized for the information most appropriate for them. That doesn't make them financial institutions doing KYC, it makes them proactively aligned vulnerability detectors and deterrents.

Treasury's OCCIP has engaged extremely constructively for years with the full range of digital infrastructure providers related to and well beyond financial institutions. Regulators and policymakers should not, as some have suggested,[34] build these guardrails by forcibly importing intermediaries into crypto systems[35] any more than it would make sense to require telephone companies to have switchboard operators again to affirmatively verify the identity of who is using any given phone. Rather, to align with the ways in which illicit finance risks in technology systems in the financial services sector are handled today, much of crypto infrastructure should be addressed and assisted by OCCIP in their natural alignment.

---

[33] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4607332

[34] The Bd. of the Int'l Org. of Sec. Comm'ns, Policy Recommendations for Decentralized Finance (DeFi) Consultation Report, 22 (2023), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD744.pdf ("A regulator should aim to identify the natural persons and entities of a purported DeFi arrangement or activity that could be subject to its applicable regulatory framework (Responsible Person(s))."").

[35] Carla Reyes, *Law's Detrimental Reliance on Intermediaries*, 92 Geo. Wash. L. Rev. (forthcoming 2025), SMU Dedman School of Law Legal Studies Research Paper No. 630 (2024), https://papers.ssrn.com/abstract=4692755.

OCCIP, in its own words, works with industry bodies "*to enhance the security and resilience of financial services sector critical infrastructure and reduce operational risk*" and "*to share information about cybersecurity and physical threats and vulnerabilities, encourage the use of baseline protections and best practices, and respond to and recover from significant incidents*."[36] OCCIP coordinates across law enforcement to disseminate information for effective mitigating measures for financial infrastructure;[37] and provides a conduit for actionable information exchange in these areas through its seminal role in the Financial Services Information Sharing and Analysis Center ("FS-ISAC"), a private sector not-for-profit cybersecurity intelligence sharing organization that is governed by its roughly 4,600 members focused on the financial system.[38] A similar organization could be established for crypto that includes representatives and open source developers who can help route information to the right people to assist. Much of this has been or is currently being built in the DeFi sector — notably, industry efforts for cyber-security frameworks[39] and an ISAC[40] — but the types of industry and regulatory coordination facilitated by OCCIP will further the robustness of this work.

We are not saying don't manage crypto risk. We are saying manage risk for critical infrastructure in ways we already know work, like activity-based cyber indicators, rather than treating every bytecode in data movement as a "bank" to hinge on KYC — which itself creates a false sense of security and a dangerous demand-signal for vulnerable information, including by theft or extortion. Give public and private sector actors naturally aligned around security and opportunity a chance to succeed.

Closing

My father grew up in a small coal and steel town, where his father was a justice-of-the-peace. He always said, "All that people want is an opportunity." No matter how it turns out. Just a chance at self-realization – whatever that means to them. That is how our democracy was founded, and how it stays strong, as a matter of national security – by attracting those who care deeply about each other getting a chance, in a world of authoritarians and oppressors who despise the unpredictability of distributed opportunity. That democratization, and the natural, non-coerced alignment of people around principles, is far stronger and more resilient for national security than closing off the unpredictability of opportunity.

---

[36] *Financial Institutions*, U.S. Dep't of the Treas., https://home.treasury.gov/about/offices/domestic-finance/financial-institutions.

[37] *OCCIP Issues Update on Ransomware Incident Targeting Financial Institutions*, America's Credit Unions (Nov. 15, 2023), https://news.cuna.org/articles/123316-occip-issues-update-on-ransomware-incident-targeting-financial-institution.

[38] *Information Sharing and Collaboration Issue Summary*, Bank Policy Institute (Aug. 18, 2021) https://bpi.com/information-sharing-collaboration-issue-summary/; *Multi-State Information Sharing and Analysis Center*, Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/resources-tools/services/multi-state-information-sharing-and-analysis-center (last visited Jan. 24, 2024); Crypto-ISAC, https://www.cryptoisac.org/

[39] *See* Sebastian Sinclair, *DeFi Gets a 'SEAL' Team as White Hat Hackers, Auditors Join Forces*, Blockworks (Aug. 8, 2023), https://blockworks.co/news/defi-seal-911-white-hat-hackers-auditors.

[40] *See* CryptoISAC, https://www.cryptoisac.org/.

You asked for solutions. First, give drowning agencies an opportunity to succeed through resourcing their current authorities before piling on more unfunded mandates. Second, build upon the natural alignment around shared principles of mutual empowerment to address risks together, not a deputized and weaponized but failing personal-information collection apparatus, which is the Eastern Europe my ancestors were leaving. Congress is the body that abolished slavery and enshrined civil rights. That is governing by principles and following through on promises. I appreciate all that you do to carry on that lineage with honor in public service.

Thank you for listening, I look forward to an opportunity to answer questions.