TESTIMONY OF

Michael Mosier[1]

BEFORE THE

United States Senate Committee on Banking, Housing, and Urban Affairs

"**Understanding the Role of Digital Assets in Illicit Finance**"

March 17, 2022

Thank you Chairman Brown, Ranking Member Toomey, and Members of the Committee for holding this hearing and inviting me to participate. It's an honor to be here. Congress represents the breadth of viewpoints across our society and has a critical role in reflecting and protecting the democratic foundation and personal sovereignty of the people.

My grandfather was a justice of the peace in a small mining and steel town in Western Pennsylvania. Sadly, he died long before I was born. But I treasure one of his campaign cards from a 1953 election that announces: "*Endorsed by Labor. An avowed enemy of communism*." Those juxtaposed statements encapsulate a sense of collective empowerment of the time, but also a resolute vigilance against totalitarian collectivism. They underscore the importance of maintaining a balance. Of sufficiently empowering people, organizations, and governments to prevent abuse, while ensuring checks on that power, so that it is not itself used to abuse.

A desire to protect personal sovereignty in the face of abuse led me to public service. As a new lawyer at a firm, I took on *pro bono* cases to help victims of domestic violence obtain protective orders, then wanted to do more. I became a state prosecutor at the Manhattan District Attorney and eventually a federal prosecutor at the Department of Justice (DOJ), investigating kleptocracy as well as the financing of human trafficking. Preservation of self-determination has guided me through roles as Deputy Chief in DOJ's Money Laundering Section, Director at the White House National Security Council, OFAC Associate Director, Counselor to the current Treasury Deputy Secretary, and, most recently, Acting Director of FinCEN.

From my experiences, I have seen firsthand that, yes, investigative ability is critical, including as a deterrent; but we must not confuse tools with the mission, which is to preserve the self-determination upon which our country was founded, and to empower people to be able to thrive and protect themselves. Preserving this balance requires a thoughtful approach to new technologies. If every new technology is viewed with suspicion, we risk harming the citizens we've sworn to protect. At FinCEN, we constantly invited the public for conversations, from cryptography professors, to civil society explaining how vulnerabilities are turned against people

[1] General Counsel, Espresso Systems. *Previously*: Acting Director, Dep.Dir./Digital Innovation Officer, FinCEN; Counselor (cybersecurity & emergent technology) to the Deputy Secretary of the Treasury; in-house counsel, Chainalysis; Director (transnational organized crime), White House National Security Council; Associate Director, OFAC; Deputy Chief, Money Laundering Section, USDOJ; adjunct professor, Georgetown University Law Center.

under authoritarian rule, constitutional privacy and speech experts, child exploitation and anti-corruption groups, and core developers of privacy technology. This education was nearly weekly – an obligation as public servants to ensure we reflected all the perspectives of the people we serve.

The Anti-Money Laundering Act (AML Act) [2] passed last year modernizes our approach to financial integrity, including the need to prioritize some risks over others, and to strike a balance that guarantees opportunity. That balance is also reflected in our separation of powers and our Constitution. Because no matter the best intentions, people are fallible. In thinking about self-determination, when we speak of "illicit finance," we must not forget defenders of democracy whose financing might be considered "illicit" to the autocrats and invading armies they resist. As we painfully see around the world right now, it is fundamental to democracy that people have the opportunity to protect themselves in the face of fallibility and brutality.

The same cryptographic capabilities discussed here today enabled secure, auditable humanitarian aid to 60,000 healthcare workers in Venezuela under a repressive regime, accomplishing a major foreign aid objective tied to a White House national security emergency.[3] The best way to send Office of Foreign Assets Control (OFAC)-authorized aid that would not be intercepted by the Venezuelan regime was to do it outside of their domestic banking system, through USDC cryptocurrency, and using Virtual Private Networks (VPNs).[4] No doubt the Venezuelan regime considered the use of those previously frozen assets "illicit finance," but to us they were cryptographically secure humanitarian aid.[5]

Likewise, in the past few weeks, tens of millions of dollars worth of cryptocurrency were donated by the public to Ukraine – faster and more aid than the UN provided. Further, the transparency of government-identified wallets on a public ledger is a substantial improvement in accountability from UN aid through traditional banking, like the UN Oil-for-Food scandal.[6] Streaming in 24/7, with no limited banking hours; with fewer intermediaries to be disrupted or take fees off the top; and available with a mere phone app. No doubt, the Russian government considers that money "illicit" and would stop it if they could. Resilient money is part of a duality of sovereignty that, like most things, can be considered good and bad.

For policymakers, the key is to find a balance that doesn't merely chase bad actors but also prevents exploitation of the vulnerable from the start. Having spent decades with victims of crime, I can say: you will never make them whole. Even if you get some of the money back – and rarely will you get it all back – you will never undo the trauma of being violated, exploited, and having your vulnerability exposed so concretely. We must empower people to protect themselves from exploitation, not just avenge the victims. Cryptocurrencies, like the

---

[2] https://www.fincen.gov/anti-money-laundering-act-2020
[3] https://www.circle.com/blog/circle-partners-with-bolivarian-republic-of-venezuela-and-airtm-to-deliver-aid-to-venezuelans-using-usdc
[4] https://www.ft.com/content/2a271032-35b4-4969-a4bf-488d4e9e3d18
[5] https://www.ft.com/content/2a271032-35b4-4969-a4bf-488d4e9e3d18
[6] https://www.law.nyu.edu/news/IILJ_IRAQ_OILFOOD

cryptography with which they are built, can be used in crime, but we'd be naive to think they are not also powerful tools to empower and protect the innocent.

Related to democracy and threat prevention, while briefly serving as Counselor to the current Treasury Deputy Secretary, my portfolio was cybersecurity & emergent technology in the wake of the SolarWinds cyberattack. The Russian Foreign Intelligence Service spent months inside computers across the private sector and government agencies.[7] It confirmed what we had been saying for years: that cybercrime is not just about the money. Over-attributing cybercrime to cryptocurrency misses significant operating models and preventive measures that can be taken.

Having worked on cybercrime for years, including at FinCEN and the National Security Council, here are a few of **observations about ransomware** in particular:

1. Ransomware dates back to 1989, two decades prior to the emergence of Bitcoin in 2009. Payments have come in a variety of fiat "digital" methods such as online payment processors, credit cards, and other traditional money transmission services for decades.

2. Yes, cryptocurrency has become the recent payment of choice because of the speed and its *perceived* anonymity. However, payments made in cryptocurrency offer Law Enforcement significant visibility and investigative benefits over opaque banking, as we saw with the recovery of $2.3 million in cryptocurrency from the Colonial Pipeline attackers. There are many other examples of cases being solved much faster because cryptocurrency was involved, cases where we could immediately identify on a public ledger which Virtual Asset Service Provider (VASP) to subpoena using immutable public evidence rather than years of Mutual Legal Assistance Treaty (MLAT) process and guesswork about which bank might be involved due to opaque wire transfers and shell companies.

3. The increase in ransomware payments has less to do with criminals reflecting current financial trends, and more to do with three practical emergences:

    a. First, the advent of **Ransomware-as-a-Service**, making kits widely available, regardless of coding skills, drastically reducing barriers to entry;

    b. Second, the use of **double extortion**, greatly increasing payouts by also threatening to expose stolen data, not just lock the computer; and

    c. Third, wide adoption of **cyber insurance**, which, while good in itself, also means ransomware actors know victims have ability to pay, driving up demands and payouts.

In light of these three substantial factors, it greatly oversimplifies the issue to blame "cryptocurrency" for payments increasing. Ignoring the variety of factors at play, this claim fails to recognize that part of the solution is having cyber insurance policies require that the

[7] https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

policyholder develop and maintain meaningful cybersecurity practices as one of the best ways to help reduce payments – and, importantly, reduce victims from the beginning. A ransomware attack avoided is a bigger victory than a perpetrator apprehended.

We make decisions everyday about balancing risk and opportunity to thrive. The best defense against cybercrime is disconnecting computers. But we have decided that it's better to manage risk rather than stop communicating, creating, and transacting across the world seamlessly. Likewise, we decided as a nation that although encryption itself makes it more difficult for the government in some instances to monitor activity, that security also protects people from hackers and protects human rights actors from autocrats so they can promote democratic discourse. As Sen.Wyden has said, "*Secure, encrypted communications give people the power to organize and access information that authoritarian regimes don't want seen. End-to-end encryption is life or death for people living in authoritarian countries like Russia, China, or Saudi Arabia*."[8] The democratic resilience of cryptography doesn't stop with mere messages.

If we chronically underestimate what cryptocurrencies can do for democracy, we also grossly overestimate its use in crime. For perspective, Chainalysis's 2022 Crypto Crime Report estimated **crypto** illicit finance at **$14 billion**, about **0.15%** of all transaction volume in 2021.[9] The UNODC estimates **fiat** illicit finance between **$800 billion - $2 trillion**, or **2-5%** of global GDP - that **fiat** illicit percentage is **up to 33 times** higher than crypto's percentage.[10] For scale, crypto's 2021 illicit finance number of **$14 billion** is comparable to the **$12.4 billion** lost by bank customers through **overdraft fees** alone in 2020.[11] Apples to oranges perhaps, but meaningful context in terms of *scale of impact on consumers*. Note, it is impossible to have an overdraft with crypto, because there is no double-spending. That alone is $12.4 billion back to some of the most economically vulnerable people. Not to mention mandatory account minimums that have kept roughly 3.5 million U.S. households unbanked, which crypto does not have.[12]

There is work to be done yet for cryptocurrency. There are too many exploits, rugpulls and scams. The early internet had a lot of fraud and exploits as well. You'd order something online and have no idea whether you'd actually get it. It took years to work out consumer protections, and certainly data privacy and protection remains elusive to this day. But we haven't decided to shut down the internet. We work persistently to find the balance and prioritize risks. As an example of the wisdom in fully exploring positive uses for edge technology before preemptively overreacting, the UK previously talked of banning The Onion Router, or Tor, browser, which was originally designed by the U.S. Naval Research Laboratory and provides multi-level encrypted access to the internet.[13] Now the BBC is broadcasting via Tor in Russian and Ukrainian to bring the free flow of information to where BBC signals have been blocked.[14]

---

[8] https://twitter.com/RonWyden/status/1499384550165725190?s=20&t=1UzXFuPo-_X4czlgMBVYSg
[9] https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/
[10] https://www.unodc.org/unodc/en/money-laundering/overview.html
[11] https://www.forbes.com/advisor/personal-finance/how-to-prevent-overdraft-fees/
[12] https://twitter.com/_amanda_fab/status/1479629264194572291?s=21
[13] https://www.bbc.com/news/technology-50150981
[14] https://www.bbc.com/news/technology-50150981

And how should we prioritize risks in the context of the Russian invasion? A senior Administration official said on background call to the Digital Assets Executive Order: "*I will say, on Russia, in particular, the use of cryptocurrency we do not think is a viable workaround to the set of financial sanctions we've imposed across the entire Russian economy and,in particular, to its central bank*."[15] Similarly, my successor as Counselor to the Deputy Secretary recently said, "*You can't flip a switch overnight and run a G20 economy on cryptocurrency*. *It's an access problem, it's a rails problem, and it's just a basic liquidity problem*. *Certainly there's going to be an element [of crypto] that's part of their playbook, but it frankly isn't at the top of the list*."[16]

Three Recommendations

If you want to tangibly impact illicit finance, here are three concrete actions you can take now:

1. First, pass the **budget** that was due last October. Fifteen months after the passage of landmark AML modernization legislation, none of the tens of millions of dollars needed to implement it has been appropriated. Under a Continuing Resolution, FinCEN and OFAC are without the roughly **$74 million** increase for personnel and technology, while more and more are demanded of them.[17] Empower FinCEN to use the data already coming to them before burdening them – and industry – with additional data collection for which they will be asked what good use they made of it. They are being set up for failure by unfunded mandates.

2. Second, resource and expansively clarify the AML and Kleptocracy **whistleblower programs**. The **AML Whistleblower** Program should explicitly include **sanctions evasion** and **any violation of money laundering** laws in 18 U.S.C. § 1956, not just BSA violations, so that everyone is clear to crowd-source leads related to corruption and abuse, and that it is "**administrative"** forfeiture amounts that are excluded from awards. Also, provide the separate **Kleptocracy Whistleblower** Program with dedicated funds and much higher caps, for the people risking their lives under autocratic regimes. Not resourcing whistleblower programs is doubly bad because it sets them up for failure, which undermines the whole system of people who want to help — from whistleblowers to overburdened public servants.

3. Third, reduce global **regulatory arbitrage**. According to Chainalysis, crypto money laundering activity is "heavily concentrated…at a surprisingly small group of services," which we know to be foreign, high-risk, centralized exchanges.[18] With limited resources, we must prioritize. Help the diligent U.S. exchanges working hard to do things right. Further, until there are **global registration standards** to identify trusted exchanges to send personal information, industry cannot implement the Travel Rule. Congress should press U.S. FATF representatives to focus on **standardized licensing across jurisdictions**, instead of FATF

[15] https://www.whitehouse.gov/briefing-room/press-briefings/2022/03/09/background-press-call-by-senior-administration-officials-on-the-presidents-new-digital-assets-executive-order/
[16] https://twitter.com/aredbord/status/1500116597607915527?s=21
[17] https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=407592
[18] 2020 Chainalysis Crypto Crime Report, p.10.

developing new, expansive definitions of “Virtual Asset Service Provider” that include software developers in a way that FinCEN cannot implement under our Constitution.

In closing, thank you again for this opportunity. Conversation is the fastest and most democratic way to ensure we are not underestimating or overestimating nuanced risks and opportunities. That is also the value of robust Notice & Comment periods for rulemakings, for which I argued strenuously with Secretary Mnuchin around the rushed wallets rulemaking that I opposed. We cannot claim to know more than all of the public. That is not how we best protect and empower. Your invitation shows dedication to discourse, and I am so grateful.

Our President issued an Executive Order last week that lays out an ambitious and thoughtful approach to empowering innovation to increase the innovative resilience and economic strength of our country – clear national security goals. All I ask is that you give our nation and president that chance to complete the studies so that we are clear on opportunities and real risks before rushing ahead of the smart and dedicated public servants working hard for years to protect and empower our country’s and the world’s democratic values. We compete with China and Russia through the power of ideals and democratic freedom that show the world what is possible such that they want to join us. Democratic discourse and personal sovereignty are foundational to our country. And, as we see in the unified solidarity with Ukraine, principles are a key national security defense in the global battlefield of ideas and ideals.

I will end with a quote engraved at the **National Memorial for Peace and Justice**, informally known as the National Lynching Memorial, to remind us that personal sovereignty requires vigilance, and that we always need a dynamic tension of personal empowerment in relation to the potential for politically-sanctioned injustice, which is hardly far in our rearview mirror. Thinking also, in his own personal, local way, of my grandfather, who as justice of the peace got up everyday knowing that justice is a constant struggle for many. And of course thinking of so many people around the world living this right now, and our obligation to do better:

For the hanged and beaten.
For the shot, drowned, and burned.
For the tortured, tormented, and terrorized.
For those abandoned by the rule of law.
We will remember.
With hope because hopelessness is the enemy of justice.
With courage because peace requires bravery.
With persistence because justice is a constant struggle.
With faith because we shall overcome.”[19]

Thank you.

[19] https://ideas.ted.com/this-is-sacred-ground-a-visit-to-the-lynching-memorial-in-alabama/