Update from the U.S. Treasury Department – Countering Illicit Finance, Counter-Terrorism, and Sanctions Evasion
Senate Banking, Housing & Urban Affairs Committee Hearing
April 9, 2024
Deputy Secretary Adewale O. Adeyemo
U.S. Department of the Treasury
Written Testimony

Chairman Brown, Ranking Member Scott, and members of the Committee, thank you for the invitation to join you here today.

As you all know, the Department of Treasury—alongside our colleagues across the U.S. government—have committed to using our tools to protect our national security. Today, I'm grateful for the opportunity to talk with you about the ways we can continue driving this work forward.

As we take steps to cut terrorist groups and other malign actors off from the traditional financial system, they look for innovative ways to move resources. Over the past several years, we have seen terrorist groups trying to take advantage of innovations in cryptocurrencies. For example, five years ago, al-Qaeda and affiliated terrorist groups, largely based out of Syria, operated a bitcoin money laundering network using social media platforms to solicit cryptocurrency donations. After receiving virtual currency, they laundered the proceeds through various online gift card exchanges to be able to purchase what they needed to advance their violent agenda.

More recently, over the past year, we have seen the Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) transfer cryptocurrency to Hamas and the Palestinian Islamic Jihad (PIJ) in Gaza. In addition, we have seen Hamas use virtual currencies to solicit small-dollar donations, and we have been able to take action against these networks.

Our problem is that actors are increasingly finding ways to hide their identities and move resources using virtual currency. What has always been true is that terrorists and other malign actors seek new ways to move their resources in light of the actions we are taking to cut them off from accessing the traditional financial system.

Today, because of the authorities Congress has provided us, we have a long track record of taking action to make it harder for these groups to use the traditional financial system to move money. We continue to use our authorities aggressively to cut off the illicit finance networks that enable illicit actors worldwide, including Hamas and other Iran-backed proxies, Russian oligarchs, and ISIS, to name a few.

The more effective our targeting has been, the more reason there is for these terrorist groups to look into virtual assets. And, to be clear, it's not only terrorist groups, but state actors like the DPRK and Russia as well.

The DPRK, which through numerous complex state-sponsored cyber heists, is able to acquire, launder, and store illicit revenue. It relies on anonymity-enhancing technologies like mixers to hide the sources of its funds. And it leverages over-the-counter digital assets traders to acquire

fiat currency. In addition, we've seen Russia increasingly turning to alternative payment mechanisms—including the stablecoin tether—to try to circumvent our sanctions and continue to finance its war machine.

While we have had some success in rooting out illicit finance in the digital asset ecosystem, we need to build an enforcement regime that is capable of preventing this activity as more terrorists, transnational criminals, and rogue states turn to digital assets. That's why we sent the Committee proposals to strengthen counter-terrorist financing authorities, and we look forward to working with the Committee on your ideas and proposals.

The options I sent over to the Committee in November focused broadly on three reforms. The first is the introduction of a secondary sanctions tool targeted at foreign digital asset providers that facilitate illicit finance. Today, Treasury has authorities that enable us—in many cases—to prohibit U.S. correspondent accounts and transaction processing for foreign financial institutions that have operated with a designated person. These authorities have enabled us to disrupt high-priority illicit finance streams in Russia, Iran, and North Korea. But, unlike banks, foreign cryptocurrency exchanges and some money services businesses do not have or depend on correspondent accounts for all of their transactions. A new secondary sanctions tool would help Treasury to evolve its targeting capabilities and would account for the technological changes that have rendered highly effective tools in traditional payments contexts less effective against virtual currencies.

The second reform centered on modernizing and closing gaps in existing authorities by expanding their reach to explicitly cover the key players and core activities of the digital assets ecosystem. Entities such as virtual asset service providers (VASPs) and cryptocurrency exchanges didn't exist when the BSA and IEEPA were enacted, but we know that today, they play a major role in how currency moves digitally and should be regulated as such.

Finally, a third reform addresses jurisdictional risk from offshore cryptocurrency platforms, which is a key challenge. By reforming existing authorities, we can clarify that our authorities can reach extraterritorially when digital asset entities harm our national security while taking advantage of our financial system. This will also promote a level playing field for U.S.-based VASPs.

There is clear overlap between these proposals and the bills coming out of this Committee. We agree that the use of these emerging technologies by illicit actors can have impacts on the national security, foreign policy, and economy of the United States. That's why the United States has a strong interest in ensuring that our tools and authorities are available and ready to mitigate the risks in this quickly evolving ecosystem, including for dollar-based digital assets in particular.

As you know, my team has been actively involved in providing technical assistance on these topics and we are working to find solutions that balance the threat, our current capabilities, and where we may require additional authorities. The Treasury Department is eager to continue working together through the details of this Committee's proposals. We all share the common

aim of ensuring that in the pursuit of technological innovation we do not disregard the safeguards that instill trust and reliability in the U.S. financial sector.

While we continue to assess that terrorists prefer to use traditional financial products and services, we fear that without Congressional action to provide us with the necessary tools, the use of virtual assets by these actors will only grow. We are grateful for the partnership of Congress and this Committee in helping Treasury root out illicit finance from the U.S. financial system and to hold illicit actors accountable. I look forward to today's discussion on how we can continue this work.