U.S. DEPARTMENT OF THE TREASURY

Remarks by Assistant Secretary Elizabeth Rosenberg at the Crypto Council for Innovation

November 18, 2022

As prepared for delivery

Thank you to the Crypto Council for Innovation for hosting me and bringing together representatives from across industry today. My name is Elizabeth Rosenberg and I'm the Assistant Secretary for Terrorist Financing and Financial Crimes at the U.S. Treasury.

In mid-September and pursuant to President Biden's Executive Order on Digital Assets, Treasury published an Action Plan to Mitigate the Illicit Finance Risks of Digital Assets – a roadmap for how the U.S. government, led by the Treasury Department, will bring greater transparency to the digital asset sector. The report identifies seven priority actions, including improving global anti-money laundering/countering the financing of terrorism (AML/CFT) regulation and enforcement, strengthening U.S. supervision of the virtual asset service providers sector, and engaging with the private sector.

Collaborative work both with the private sector, and between private sector entities, is critical for detecting and countering illicit finance. To deepen our insight and engagement with industry, in mid-September, we released a Request for Comment, seeking feedback on the Action Plan, our assessment of illicit financing risks, and opportunities to strengthen public-private collaboration.

The comment period ended on November 3 and I want to thank industry for the all the submissions.

While we continue to review the comment letters in detail, I wanted to highlight two specific issues addressed in the comment letters: a need for regulatory clarity and more public-private engagement. Many of the comments acknowledged that in the United States, virtual asset service providers are subject to a regulatory framework for AML/CFT and have sanctions obligations. With this in mind, industry commenters identified specific areas, such as questions around decentralized finance (DeFi), where they could benefit from additional

regulatory clarity or guidance. As a matter of policy, we want to ensure that industry has a clear understanding of AML/CFT and sanctions obligations. Therefore, we will be reviewing the specific issues industry identified in the comments and explore how, whether through regulation, guidance, or outreach, we can best address industry questions and uncertainty.

Second, we received thoughtful feedback on opportunities to expand and formalize our engagements with the virtual assets industry. I recognize that industry has unique insight into illicit finance threats. Stronger two-way dialogue can also strengthen the U.S. government's understanding of technological innovations and changes, as well as create greater opportunities for industry to identify areas where these innovations may result in regulatory uncertainty.

I am here today, as part of that larger effort, to build direct relationships with industry, solicit further feedback, and learn about developments in the virtual asset ecosystem. To that end, I want to take a moment to discuss some of the policy questions surrounding our approach to mixers following Treasury's designations of Blender and Tornado Cash. We recognize that, in some instances, virtual assets may provide more insight into financial activities by virtue of public blockchains, which can be used to support AML/CFT compliance. Still, I understand that some virtual asset users may want to preserve their privacy when conducting transactions.

As was clearly stated in President Biden's Executive Order, we want to ensure that safeguards are in place to promote the responsible development of virtual assets to maintain privacy and shield against arbitrary or unlawful surveillance. The challenge is that mixers, as currently operating, provide anonymity, a way for illicit actors to obfuscate the movement and the origin or destination of funds, while reducing law enforcement's visibility into these transfers. The challenge is that while these services often operate as money transmitters and thus have regulatory reporting obligations, they may deliberately operate in a non-compliant manner to make it more difficult for regulators and law enforcement to trace illicit funds.

Illicit actors are capitalizing on these vulnerabilities. The Democratic People's Republic of Korea's (DPRK) Lazarus Group uses mixers to launder proceeds of virtual currency heists. Illicit actors also use mixers to launder proceeds of ransomware, drug trafficking, and other criminal activities. We are concerned that mixers are being abused for illicit purposes and we are therefore compelled to take action to address this risk. In the case of Blender and Tornado Cash, the Lazarus Group used mixers to obfuscate the source of funds derived from

a March 2022 cyber heist. In addition, malicious cyber actors' used the service provided by Tornado Cash to launder more than $96 million of funds derived from the June 24, 2022 Harmony Bridge Heist, and at least $7.8 million from the August 2, 2022 Nomad Heist.

The Treasury Department cannot allow such egregious activity to occur. Illicit actors are abusing mixers to launder funds. It is our goal to be clear about obligations, but we need industry to take clear steps, in line with AML regulations and sanctions obligations, to prevent illicit actors from abusing this activity. Our goal and intention is not to deter the development of technologies that provide privacy for virtual asset transfers. We welcome opportunities to further engage with industry on how these technologies can both promote privacy while also mitigating illicit finance risks and complying with regulatory and sanctions obligations.

Before I turn the discussion over to all of you, I want to thank you all for making time to speak with me today and sharing your insights. I welcome feedback and hope that we can use our time to identify how we all, government and industry, can further collaborate to promote transparency and integrity in the virtual asset ecosystem.