U.S. DEPARTMENT OF THE TREASURY

Treasury Releases 2023 DeFi Illicit Finance Risk Assessment

April 6, 2023

WASHINGTON — Today the U.S. Department of the Treasury published the 2023 DeFi Illicit Finance Risk Assessment, the first illicit finance risk assessment conducted on decentralized finance (DeFi) in the world. The assessment considers risks associated with what are commonly called DeFi services. While there is currently no generally accepted definition of DeFi, the term broadly refers to virtual asset protocols and services that purport to allow some form of automated peer-to-peer transactions, often through use of self-executing code known as "smart contracts" based on blockchain technology. This term is frequently used loosely by the private sector, often for services that are not functionally decentralized.

Actors like the Democratic People's Republic of Korea (DPRK), cybercriminals, ransomware attackers, thieves, and scammers are using DeFi services to transfer and launder their illicit proceeds. They are able to exploit vulnerabilities, including the fact that many DeFi services that have anti-money laundering and countering the financing of terrorism (AML/CFT) obligations fail to implement them.

"Risk assessments play a foundational role in promoting understanding of the illicit finance risk environment and more effectively protecting the integrity of the U.S. financial system," said, Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. "Our assessment finds that illicit actors, including criminals, scammers, and North Korean cyber actors are using DeFi services in the process of laundering illicit funds. Capturing the potential benefits associated with DeFi services requires addressing these risks. The private sector should use the findings of this assessment to inform their own risk mitigation strategies and to take clear steps, in line with AML/CFT regulations and sanctions obligations, to prevent illicit actors from abusing DeFi services."

The primary vulnerability that illicit actors exploit stems from non-compliance by DeFi services with AML/CFT and sanctions obligations. DeFi services engaged in covered activity under the Bank Secrecy Act have AML/CFT obligations regardless of whether the services claim that they currently are or plan to be decentralized. Other vulnerabilities include the potential for some DeFi services to be out of scope for existing AML/CFT obligations, weak or non-existent AML/CFT controls for DeFi services in other jurisdictions, and poor cybersecurity controls by DeFi services, which enable the theft of funds.

While risk assessments are primarily designed to identify the scope of an issue, the study also includes recommendations for U.S. government actions to mitigate the illicit finance risks associated with DeFi services. These include:

- strengthening U.S. AML/CFT regulatory supervision
- considering additional guidance for the private sector on DeFi services' AML/CFT obligations
- assessing enhancement to address any AML/CFT regulatory gaps related to DeFi services

The DeFi risk assessment builds upon Treasury's other recent national risk assessments and furthers the work outlined in Executive Order 14067 on "Ensuring Responsible Development of Digital Assets." It also includes a request for input from the private sector to inform next steps; Treasury welcomes feedback about the assessment.

Click here to read "Illicit Finance Risk Assessment of Decentralized Finance" .

###