



U.S. DEPARTMENT OF THE TREASURY

Remarks by Assistant Secretary for Terrorist Financing and Financial Crime Elizabeth Rosenberg on DeFi Risk Assessment at the Atlantic Council

April 21, 2023

As Prepared for Delivery

On April 6th, Treasury released the first ever [Illicit Finance Risk Assessment of Decentralized Finance](#) . This is the first illicit finance risk assessment conducted on decentralized finance (DeFi) services in the world. Today, I would like to address why we did this, what some of the most important findings are, and how we are thinking through our next steps in this emerging field.

There has been considerable attention to DeFi services over the past few years given the rapid growth of the sector, as well as theft from DeFi services, including some high-profile cases tied to North Korean cyber actors who not only stole virtual assets from DeFi services, but then also used DeFi services to launder the stolen proceeds. That's why in September 2022, Treasury committed to conducting a risk assessment on DeFi services as part of its [Action Plan to Mitigate Illicit Finance Risks of Digital Assets](#) .

For this risk assessment we started by defining what we mean by "DeFi," to cut through some of the amorphous and ambiguous interpretations of "DeFi" itself: we use DeFi to refer broadly to virtual asset protocols and services that purport to allow for some form of automated P2P transactions, often through the use of self-executing code like smart contracts developed on blockchain technology. We decided to take this broad approach to DeFi services to cover a range of structures and activities, and hopefully reach all current illicit finance risks in the entire DeFi ecosystem.

We spoke with scores of stakeholders to gather views for the report and asked intentionally broad questions, such as whether illicit actors are misusing DeFi services at all. Only after extensive engagement with government partners and industry did we move on to determine the steps we could take to mitigate the risks we uncovered. Our intention with this risk assessment was not to evaluate the relative merits of decentralization or centralization, but

instead to broadly consider the illicit finance risks associated with DeFi services and potential measures to address them.

The results of investigating these questions inform the basis of our risk assessment. My hope is that every person with an interest in DeFi will read the product, use it in their own decision-making, and provide substantive feedback on how the risk environment is changing as DeFi technologies advance.

Now onto our findings.

One of our primary findings affirmed what Treasury has said previously—that DeFi services often have a controlling organization behind them that provides a measure of centralized administration and governance. While I do not dismiss the potential for widespread truly-DeFi services one day, they simply are not a major feature of the current landscape. This means that when we consider DeFi services today, there are generally persons and firms associated with those services to which AML/CFT obligations may already apply.

Unsurprisingly, our assessment found that illicit actors, including ransomware cybercriminals, thieves, scammers, and North Korean cyber actors, use DeFi services specifically to launder illicit funds.

The assessment further identified several techniques that involve DeFi services in this process, including the use of cross-chain bridges to exchange virtual assets for others that operate on other blockchains; sending virtual assets through mixers, some of which claim to be decentralized; and placing virtual assets in liquidity pools as a form of layering. There has also been outright theft from DeFi services, exploiting weak cybersecurity controls within DeFi technology.

The key regulatory vulnerability identified by the risk assessment is noncompliance with existing U.S. AML/CFT obligations by DeFi services. The U.S. Department of the Treasury considers any DeFi service performing the functions of a covered financial institution to be subject to BSA obligations, including AML/CFT obligations, regardless of how decentralized the services may be. Additionally, U.S. persons, wherever located, are required to comply with U.S. economic sanctions regulations. Many DeFi services subject to these obligations are failing to comply, thereby increasing the ease of access and the potential for abuse by illicit actors looking to fund their malicious activities. While technology, and DeFi in particular, conveys a sense of impersonality, let's remember why we have AML/CFT controls in the first place: to cut

off funding for illicit actors and prevent their acts of crime and terror. There are real-world consequences of failing to uphold these regulatory obligations.

So where are we going now?

The first recommendation I want to focus on is to continue to strengthen U.S. AML/CFT supervision of virtual asset activities in tandem with considering additional guidance for the private sector on DeFi services' AML/CFT obligations. Additionally, we will assess enhancements to our domestic AML/CFT regulatory regime as applied to DeFi services and monitor responsible innovation of AML/CFT and sanctions compliance tools. This is where I want to offer a specific message to the private sector. "DeFi innovation" should not only occur in the technical, financial domain—there is an enormous need and potential for innovation in compliance mechanisms that could help all players in the digital ecosystem ensure they remain on the right side of the law and that they are not facilitating the funding of criminal or terrorist networks.

We are keenly invested in having and sustaining these discussions with the private sector. Not only are we interested in encouraging responsible innovation and the development of emerging technologies, we also recognize the need to adapt as the technology advances. This is why we have been and will continue to emphasize public-private engagement and collaboration for emerging technologies in general and for DeFi services in particular.

Just last week, members of my team presented the findings of our risk assessment during the Financial Action Task Force (FATF) Virtual Assets Contact Group meeting in Tokyo. Over 100 participants from over 18 countries and 30 private sector firms discussed how the FATF standards apply to DeFi services, in both a government-only session and a session with members of the private sector.

For those of you who have already looked through the risk assessment, you may have seen that the report deliberately poses questions to its readers to ensure we keep this feedback loop going. We need your perspective on how we can best encourage DeFi services to comply with existing AML/CFT and sanctions regulations, where we should clarify obligations, and how we can ensure that DeFi services falling outside the scope of current regulations are not open for exploitation by illicit actors.

With that I look forward to hearing from you with feedback on the report, the DeFi landscape as it is now, and how we can all play a role to protect the financial system from abuse.