***THE CRYPTO EXCHANGE*: ANALYZING THE TREASURY'S ILLICIT FINANCE RISK ASSESSMENT OF DECENTRALIZED FINANCE**
HOST: ETHAN OSTROFF
GUESTS: MIKE LOWE AND MATT ORSO

Ethan Ostroff:

Welcome to another episode of The Crypto Exchange, a Troutman Pepper podcast focusing on the world of digital assets. As longtime leaders in the intersecting worlds of law, business, and government regulations, our lawyers can go beyond the buzzwords and headlines to make sense of the emerging legal and regulatory frameworks for operating in the digital asset industry. My name is Ethan Ostroff, the host of the podcast and a partner here at Troutman Pepper. Before we jump into today's episode, let me remind you to visit and subscribe to our blogs, consumerfinancialserviceslawmonitor.com and troutmanpepperfinancialservices.com. And don't forget to check out our other podcasts on troutman.com/podcast.

We have episodes that focus on trends that drive the payments industry, consumer financial services writ large, the Fair Credit Reporting Act, and more. Make sure to subscribe to hear the latest episodes. Today, I'm excited to be joined by my partners, Mike Lowe, and Matt Orso, to discuss the Department of Treasury's Illicit Finance Risk Assessment of Decentralized Finance, which discusses how illicit actors are abusing decentralized finance services as well as vulnerabilities unique to DeFi services. Mike and Matt really excited about today's discussion. I guess just to set the stage, this assessment signals that Treasury intends to increase its focus on the DeFi sector and expects DeFi market actors to integrate anti-money laundering and countering the financing of terrorism compliance into their services.

The assessment indicates its findings will inform efforts to identify and address potential gaps in the United States' AML, CFT, regulatory, supervisory, and enforcement regimes for DeFi. And it seems like the assessment makes clear that a DeFi service that functions as a financial institution as defined by the Bank Secrecy Act must comply with the BSA's AML CFT requirements. I think one of the things I noted from looking at this assessment was that it says, "The degree to which the services decentralized has no bearing on these obligations, and the automation of certain functions through smart contracts does not affect the obligations." I thought as a way to jump into this conversation, we might just start with what are they talking about when they're referring to decentralized finance or DeFi.

Mike Lowe:

Decentralized Finance, which we call it DeFi for short, it's really just a type of banking or financial services that doesn't use a traditional bank and traditional money. And traditional money is what we call fiat currency. So, instead, DeFi uses digital assets and peer-to-peer or what we call P2P payments, and it does that through blockchain technology.

DeFi typically operates through something called smart contracts, which are really just pieces of code that are executed on the blockchain. And DeFi services use these smart contracts to provide the types of services that traditional financial institutions would provide, such as asset exchange, lending, borrowing stable coins, trading, and even investments that could provide a return, among other things.

Matt Orso:

I think, in its simplest sense, think about if I've just got cash and I'm going to hand it to Mike, Ethan, and that would be what DeFi, I think, aspires to be with digital assets. Although, you can't just hand somebody a digital asset, so you need some type of mechanism, which is a blockchain, and some type of smart contract to govern the rules regarding that transfer.

Ethan Ostroff:

Sure, I appreciate that. So, I guess, guys, let's just start off maybe perhaps with some of your biggest takeaways from Treasury's assessment. Maybe Mike, your thoughts first.

Mike Lowe:

Sure. What jumped out at me when I read this was really that it didn't say much that people who operate in this space didn't already know. I mean, some of the things it talked about were that DeFi services often don't follow the Bank Secrecy Act. Yeah. Like I said, people who operate in this space sort of know that. And as a result, the DeFi services often don't comply with the AML and CFT laws and regulations. The assessment made the point that illicit actors are using DeFi to launder money. Again, that is not any great big disclosure. They do that in part because there's a high level of anonymity with using DeFi services.

They also indicated in the assessment that they've found that DeFi services are vulnerable to hacking, which is not surprising because a lot of these DeFi services are small startups. And the amount of money, time, and effort you need to put into security features to prevent hacking is something that can be lacking. The assessment also talked about how North Korean state-sponsored hackers are exploiting DeFi's vulnerabilities, and the biggest point which is that it remains unclear just which DeFi services are financial institutions within the meaning of the BSA. And the assessment noted that this ambiguity is a problem and it needs to be addressed.

Matt Orso:

And I'll just pick up along that last point that Mike noted, which is that this is a real preliminary type of a document, this risk assessment, it's obviously not a regulation or a rule, it's not even a notice of any type of a proposed rule. It's really just Treasury's initial take at assessing potential risks, illicit finance risks of the DeFi space. One thing to its credit that Treasury does mention is that they put things into perspective in terms of the scale of this. They mentioned that, in January of this year, nearly $30 billion in daily virtual asset activity occurred.

DeFi exchanges accounted for only 3% of that volume. And so, it's not that Treasury is saying DeFi is the biggest potential AML risk out there. You'll note also other literature that says digital assets make up somewhere less than 10%, quite less than 10% of all money laundering that goes on. And so, 3% of 10% is pretty small, right. But at the same time, you've got pretty large actors like the DPRK in North Korea that Mike mentioned, that Treasury points to as well as other pretty large bad actors moving large sums of money through DeFi. So, it's not something that Treasury is going to ignore by any means.

Mike Lowe:

Yeah, that's a great point, Matt. I think it's absolutely spot on that most money laundering is still going to be done with traditional money with fiat currency. This is an assessment really just to get DeFi services on the radar of the public, almost like a way to start putting DeFi services

themselves on notice that Treasury is really interested in trying to come up with a way to fix the problems that it is putting pen to paper about.

Matt Orso:

The thing I've really struggled with in reading this risk assessment is the BSA and AML laws and regulations were originally designed without the notion of virtual assets in mind. And so, they focus on the obligations of actors like business entities and individuals. When we're talking about DeFi, we're really, in a lot of cases, talking about code or blockchain or smart contracts or protocols. And so, that's one of the points I think that Treasury is struggling with when they talk about DeFi, and they're very careful to call them services, right.

Not DeFi companies or not DeFi businesses. They call them DeFi services. At what point do they become, quote-unquote, financial institutions and subject to these AML laws? They do get into a good bit on the fact that there are a lot of services out there that would purport to be DeFi, but that if you really kind of peel back the onion a bit, there are some pretty centralized actors with certain levels of authority that would constitute some at least semblance of centralization as opposed to decentralization.

Mike Lowe:

And Ethan, to put a final point on your first question, which was about the big takeaways, my other big takeaway on this is that this is really a lot of issue spotting and flagging of problems without really any solutions or even firm suggestions on how to fix things. I mean, there are suggestions on things that need to be done, but it's really things like engaging with industry to provide better guidance on the applicability of the BSA to DeFi services. The assessment talks about closing the gaps in the BSA to make more DeFi services fall within the definition of a financial institution, but it doesn't really point to what specific gaps it's talking about, and it doesn't suggest how to close them.

So, the other suggestions are things like, "Hey, the need to increase engagement with foreign partners to push for international standards and the suggestion of promoting innovation in the industry by providing grant money to get industry to develop tools that could incorporate AML and CFT compliance into the DeFi services code." The problem is going to be that, as the assessment acknowledges, a lot of DeFi services have no interest in complying with AML CFT regulations. They don't even think that they're subject to jurisdiction in a lot of instances where they should have to comply. So that's going to remain a challenge.

Matt Orso:

Yeah, I think to your point, Mike, one of the core reasons why DeFi even exists is to not have to comply with those laws and regulations so that individuals can transact with digital assets in a more private or pseudonymous manner without having to disclose who they are to the world. One of the other big takeaways that I took is something that's not in the risk assessment document.

But I think it's something that some in the industry have raised, and I think is important to consider, probably more from a policy perspective when Congress gets to actually making laws on this front, and that is if we're going to push DeFi to comply with BSA AML rules, a big part of that is collecting customer information, knowing your customer. The question is, the way that the industry is now, there are quite a few gaps from a cybersecurity perspective.

So, do you really want DeFi exchanges at every level gathering and keeping lots of very sensitive customer information when they aren't yet up to speed or up to snuff on their cybersecurity defenses? So that could create maybe unanticipated very significant risk for additional types of crime.

Mike Lowe:

That's a good point.

Ethan Ostroff:

Very interesting. So, what do you guys see as the biggest issue identified in the assessment by Treasury?

Matt Orso:

I think Mike already hit on it. It's that there's this whole industry out there that's growing at a pretty rapid clip, and that's varied. Any given DeFi service can be a wholly different creation, and a different fact pattern, and a different level of authority or decentralized nature.

The biggest takeaway is Treasury sees the need to regulate in this area to curb money laundering and terrorist financing, and it's trying to get its arms around how to do that and how to do that effectively, how to do that efficiently, and I think it's, to its credit, seeking industry input on what that really looks like.

Ethan Ostroff:

Part of the question becomes though, who's the industry, right?

Matt Orso:

Yeah. Yeah.

Ethan Ostroff:

Part of this whole idea is it's built around peer-to-peer transactions without a trusted intermediary, right. So, who's the industry? And it also, I mean, seems like this is part and parcel of the White House report last year asking for Treasury and other federal financial regulators to undertake certain activities and engage in certain types of research and produce reports.

And they're getting... Treasury, and the White House, and other federal regulators are getting pushed by members of Congress who believe there is a huge problem in the DeFi space in a number of ways, but in particular, within the context of money laundering and financing of terrorism.

I think of particular Senator Warren, who's been very active on this front, and there's a bunch of pending legislation on the Hill right now that's at least in part intended ostensibly to help try to fill some of the gaps in the AML CFT compliance world. Mike, you mentioned earlier your experience as a federal prosecutor. Can you give us some idea or your take on how illicit actors use DeFi to affect money laundering?

Mike Lowe:

One of the things that I had seen when I was prosecuting cases was that the ability to exchange one type of virtual asset for another that's easier to use or is less traceable is one of the

advantages of using these DeFi services. You can go through a decentralized exchange. You can use cross-chain bridges, which basically allow users to exchange virtual assets from one blockchain to another. And when you do that, you start obfuscating the funds that you're trying to launder, and in this case, the funds are digital.

There's also the issue of mixers, which are very good at obfuscating the source or the destination or even the amount of the illicit proceeds because they typically pool or aggregate virtual assets from multiple individuals. And for the most part, mixers are not following any AML CFT compliance regulations obligations. And in fact, they often advertise that they don't do that, and they advertise that they don't cooperate with law enforcement.

As Matt pointed out earlier, part of the biggest issue is when you don't have your customer protocols in place, and you're allowing this level of anonymity in the DeFi space, it's going to be very attractive to illicit actors. And Treasury acknowledges that. There's not a lot they can do about it right now, and so they're sort of flagging the issues and trying to get this on people's radars, what I think.

Ethan Ostroff:

This is not inconsistent, I don't think, with what we see going on at an international level, with what we're hearing from the IMF, what we're hearing from the G-20, right, in efforts to engage in cooperation amongst many states internationally to try to understand how they can go about bringing people in the DeFi space into the AML CFT type regimes in an effort to coordinate that internationally to try to close the gaps on places where, for example, illicit mixers are able to operate from and avoid cooperation with law enforcement and avoid various types of law enforcement activities. What do you guys see sort of looking at on the horizon as far as enforcement activity that might attempt to force DeFi actors to comply with AML CFT obligations in the United States?

Matt Orso:

Treasury does, in the risk assessment, identify some of its thinking as far as this goes? It gives some examples from historical CFTC and SEC actions. The risk assessment doesn't get that specific, but it does suggest that individuals who participate in the decentralized autonomous organization or DeFi governance process, they could be deemed to be members of an unincorporated organization and then subject to enforcement for that association's legal violations. So, they have different ways of potentially targeting individuals who have some semblance or level of control of a DeFi framework or service.

I think that's really where they're going to start. If there's going to be enforcement in that way in the DeFi space, it's those types of individuals who might be the subject of enforcement. Those who have some type of concentrated voting rights in the structure of the DeFi service, possibly the innovator or the early adopters, who hold the largest amount of tokens for that DeFi service. I think there are different ways that you could look to determine who has, quote-unquote, authority, which then indicates that it might be more centralized than it purports to be.

Mike Lowe:

And I'll add Ethan. From what I've seen and what I expect to go forward is that CFTC will continue to bring actions. They'll bring civil enforcement actions, but there's only so much they can do, particularly given the ambiguity over which DeFi services are financial institutions under the BSA. And so, I think what we'll see is that the enforcement actions they bring are going to

be pretty limited to really clear-cut cases where they have jurisdiction, and they believe it's a very easy case to prove that the DeFi service is covered by the BSA.

I think with respect to DOJ and criminal enforcement, we're going to continue to see what we've seen in the crypto space in general, which is something you and I have talked about on a previous podcast, and that is that DOJ really won't bring criminal enforcement actions unless we're talking about a clear fraud case. And when that happens, it's going to be, in all likelihood, a wire fraud case. I mean, if you look at the historical enforcement actions that the DOJ has brought, that's what you see. There was even a pretty recent case out in my old district, the Central District of California. Le Ahn Tuan was charged with wire fraud and money laundering conspiracy back in June of last year.

And this was basically a fraud scheme, what they call a rug pull scheme involving a non-fungible token called the Baller Ape, which putting aside the fact that it involved this token, it was really a case where somebody set up a website to get money, and then they deleted the website and stole the money. And then they laundered it through chain hopping, and they got about 2.6 million, was the allegation. So that kind of case is what I think you'll continue to see from DOJ on the criminal side of things.

I think you'll see the SEC continue to get aggressive just like they have been when it comes to defining a particular asset as a security, even if it's a virtual asset. And I also think we're going to start seeing more OFAC sanctions being applied to DeFi services because I think the reach of the OFAC sanctions is going to be a little bit broader than the reach of the Bank Secrecy Act.

Matt Orso:

Another tool that I think government has in this space that it doesn't traditionally have in the AML space is that a blockchain is almost always a public ledger. And so, the general public, including the government, can see everything that's on that ledger. And so, it has the ability through blockchain analysis, and there's a whole industry cropping up around just the analysis of blockchains and some companies that are really good at it.

Just by looking at a certain DeFi's chain, the government could likely determine what percentage of illicit finances occurring within one DeFi service versus another. And so I think that's another potential avenue if you're looking for a DOJ type of an action where it could potentially begin is if they see that this DeFi service has, it looks like it's about 80% illicit finance versus 5%, 3% over here in this other corner. That's another tool, I think, that law enforcement has and will likely use that it doesn't have in the traditional context of private bank accounts.

Mike Lowe:

That's a great point, Matt.

Ethan Ostroff:

Clearly, it's going to be very interesting to see if there's something done on the Hill legislatively. And note to our listeners. We'll be talking in an upcoming podcast about the pending legislation that's floating around the Hill and what people might expect to see from that in the next six to eight months, including whether or not there will be an attempt to amend the Bank's Secrecy Act in a way that alters the current definition of financial institution to try to explicitly bring more DeFi actors and servicers within its explicit statutory definition.

You guys mentioned earlier this idea of vulnerability to hacking, and there's certainly been a lot reported about various types of hacks at various types of amounts for years in the DeFi space,

Treasury seems to think that DeFi services are particularly vulnerable to hacking. Did they talk about why?

Mike Lowe:

Yeah, they did. In fact, one of the things that the assessment pointed out was that DeFi use cross-chain bridges, and those are often targeted because they have a central storage point that's vulnerable. They also talked about the code. And we mentioned this a little bit earlier, how a lot of these DeFi services are smaller startups, and so they don't have sufficiently secure code. One of Matt's other points about the sort of public nature of the code is something that Treasury actually talked about as one of the vulnerabilities of DeFi because some DeFi services make their code public. I'm not just talking about the blockchain, right. And if it's public, hackers can analyze it and look to exploit it.

So, these reasons, the poor cybersecurity is one of the reasons that you see DeFi services being targeted. I think part of my read on this, the sort of subtext that I get from it, is that Treasury wants people to start being a little nervous, so to speak, about having their assets in DeFi and make them aware that, "Look, you want to put your money here? This is a place that money gets stolen from." I mean money, I'm using the term money, but we're talking about virtual assets. There may be a little bit of trying to warn people away from it because of the concerns about illicit actors using the space, but yeah, I could just be reading into it.

Ethan Ostroff:

Thanks, Mike. That's super helpful. I guess, finally, the assessment talked about and posed five questions and is seeking public input on those questions. Thought you might just briefly summarize what they're asking for and why. And I guess my sense is they're asking for that input as part of a process of trying to go back to the Hill and to the White House, for that matter, and explain from the Treasury's perspective what additional laws or regulations need to be in place to address the concerns there are with respect to AML CFT in the DeFi space.

Matt Orso:

Ethan, Treasury poses five questions at the end of this risk assessment. I think we could have probably about 10 podcasts just discussing those questions. They're pretty expansive. But I think, in a nutshell, they really seek to obtain input on a few key points, at least from Treasury's perspective. One is they want to know what are the factors it should consider to determine whether or not a DeFi service is a financial institution and subject to the BSA. So that's the big question. What can be well-defined factors that are public that everyone knows, and that there's no question that if these factors are present, then it is a financial institution and subject to the Bank Secrecy Act?

On the flip side of that, they also posed the question, "Okay, let's say that a DeFi service is not a financial institution. How can government still encourage these non-financial institutions to combat illicit finance and mitigate illicit finance risks even if they're not subject to the BSA?" That's a good question. I don't know that they'll get any really good answers to that, but I think we'll find out. Those are two of the questions. The third one is it notes that non-compliance by covered DeFi services with the AML rules might be partially attributable to a lack of understanding of how these regulations apply to their services. It asks if there are additional recommendations for ways to clarify and remind DeFi services that fall under the BSA definition of the regulatory obligations. To me, this is a question that almost answers itself. It's suggesting that there are certainly DeFi services that fall under the BSA definition of financial institution.

Are there additional recommendations for ways to clarify that and remind them? I think Mike hit upon it earlier. I think laws need to be enacted that clearly define what is and is not subject to that law. That's another question they pose. The last two. One is, how can the regulatory framework effectively mitigate the risks of DeFi services that currently fall outside the BSA definition? Again, it's similar to some of these other questions. And then, finally, how should AML obligations vary based on the different types of services offered by DeFi services? And I think this is one where they'll probably get quite a few responses because there are many different types of services and DeFi players in this space.

Ethan Ostroff:

Thanks, Matt. Do you guys know, is there a deadline by which people can provide input on these questions?

Matt Orso:

I don't believe there's an official deadline, Ethan. Treasury notes that those questions will be considered as part of the recommended actions in the risk assessment and welcomes input on those questions. It doesn't have any type of a deadline, though, for when they should be submitted or even really how they should be submitted.

Ethan Ostroff:

Very interesting. Kind of unusual as well.

Mike Lowe:

Yeah, Ethan, I have to say the fact that the assessment closed with a series of questions definitely odd, and it sort of solidified my initial take on it that this was really just an attempt to look at an issue and flag other issues. It was basically a good giant issue-spotting exercise to get stuff on people's radar, and now they're asking for comment to help them come up with solutions. Very unusual, but I think that's where we're at.

Ethan Ostroff:

Got you. Well, guys, really appreciate your time and your thoughts today on this very interesting assessment by the Department of Treasury. I want to thank our audience for listening to today's episode. Don't forget to visit our blog, consumerfinancialserviceslawmonitor.com and troutmanpepperfinancialservices.com, and subscribe so you can get the latest updates. Also, make sure to subscribe to this podcast via Apple Podcast, Google Play, Stitcher, or whatever platform you use. We look forward to next time. Thank you.