The Crypto Exchange — Unpacking the Fifth Circuit's Landmark Tornado Cash Decision
Host: Ethan Ostroff
Guest: Pete Jeydel and Matt Orso
Air Date: January 16, 2025

Ethan Ostroff:

Welcome to another episode of *The Crypto Exchange*, a Troutman Pepper Locke Podcast, focusing on the world of digital assets. I'm Ethan Ostroff, the host of the podcast, and a partner here at Troutman Pepper Locke.

Before we jump into today's episode, let me remind you to visit and subscribe to our blogs, ConsumerFinancialServicesLawMonitor.com, and TroutmanFinancialServices.com. Don't forget to check out our other podcasts on troutman.com/podcasts.

Today, I'm joined by my colleagues, Pete Jeydel, and Matt Orso to discuss the recent landmark decision from the Fifth Circuit and the Tornado Cash decision, as most people were either turning off their laptops and hunkering down for Thanksgiving, or starting to travel, or do all the other things that folks were doing that week. We got this interesting decision from the Fifth Circuit, and at a high level, the court ruled that OFAC exceeded its authority by sanctioning immutable smart contracts created by Tornado Cash.

Very interested to talk with Pete and Matt about this today. Obviously, ruling is still subject to appeal, has significant implications for the use of the International Emergency Economic Powers Act in regulating DeFi technologies and the way the court, I think, went about its analysis and focus on, amongst other things, how to define property.

So, Pete and Matt, thanks for joining me today. I thought, Matt, maybe you could just start, if that's okay, talking a little bit about the background of the Tornado Cash decision and sort of how we got here.

Matt Orso:

Thanks, Ethan. It's great to be here again. Tornado Cash is what is now largely defunct cryptocurrency privacy protocol. In August 2022, OFAC sanctioned Tornado Cash despite the view of many in the industry that Tornado Cash is a fully decentralized autonomous protocol. Some Tornado Cash users challenged those sanctions in various courts. One of those cases recently went up to the Fifth Circuit Court of Appeals, which my partner Pete Jeydel will discuss in just a minute. Before we get there, I think it might be helpful to give just a high-level summary for those who need a bit more background on crypto mixers in general, and so I'll just do that briefly.

Crypto mixers, which are also known as tumblers and go by a couple of other names as well, these are services that are designed to enhance the privacy and the anonymity of

cryptocurrency transactions. So, they work by pooling together multiple transactions from various users and then redistributing those mixed coins to the participants. This process, it makes it difficult to trace the original source and the destination of the funds, and it obscures the transaction history. People use these services for related reasons, but it's mostly for anonymity and for privacy.

Anonymity, you mix coins from different users. The mixers break that link between sender and recipient, and it makes it challenging to trace that transaction path. Privacy, it provides an additional layer of privacy for those users who want to keep their financial activities confidential. Tornado Cash specifically, it describes itself as a fully decentralized, non-custodial protocol for private transactions on the Ethereum blockchain. So, it works in a pretty basic, well, it's a complex platform for sure and protocol, but it works in a high-level basic way of, you've got deposit where users deposit a specific amount of, let's just use ether, it's Ether, ERC tokens, 20 tokens. They deposit these into a Tornado Cash smart contract. The smart contract then pools the funds with those of other users. Then you've got the withdrawal part, which users can withdraw the mixed funds to a new address, which breaks the link between the original deposit and the withdrawal address.

So, I'll turn it over now to Pete so he can get a little bit more into the specifics of this Fifth Circuit appeal, and then maybe we can talk a bit about some of the criminal prosecutions and other related activity.

Pete Jeydel:

All right. Thanks a lot, Matt. Ethan, thank you for having me. I'm a brand-new partner here at Troutman. I'm really excited to join the team here. I am at heart an OFAC nerd. I am export controls, economic sanctions, attorney. So, when this Tornado Cash decision came out, it really made waves in the OFAC bar, in the National Security regulatory bar more generally. It's a fascinating decision, and you can see that reflected in the way people talk about it. There are those who say, “This is a landmark case. It's going to change the future of OFAC practice and regulation and enforcement in big ways going forward.” There are people who say, “This decision just states the obvious. It's really not very interesting. It doesn't really – may not have much of an impact.” There's a big divide in how people view the case. So, we'll dig into it a little bit.

Again, so this was a case brought by a bunch of users of the Tornado Cash protocol, people based in the US. They said, OFAC went beyond its statutory authority and imposing these sanctions. We are users of this protocol. We have the right. We have a need for privacy-enhancing services like this, for political contributions, anonymity, if you want to contribute to causes in Ukraine and you don't want the Russian government to see that. They say, “OFAC can't sanction Tornado Cash as a whole. We are US persons and we want to be able to use this mixer in transactions that have nothing to do with North Korea, which that's the reason that OFAC gave for sanctioning Tornado Cash or ransomware, cyber heists. We're conducting innocent transactions. We have the right to do that, kind of at a high level.”

And then they got into with the courts a lot of technical detail. Essentially, the claim was, again, OFAC exceeded its statutory authority in imposing these sanctions, and the statute, as you guys referenced earlier, is IEEPA, the International Emergency Economic Powers Act, the 1970s-era

statute that gives OFAC very broad authority to impose sanctions and blocking orders on the property and property interests of foreign persons based on a national emergency declaration. These users came to the court and said, “First of all, tornado cash is not even a thing. The legal term is it's not a person, it's not an individual, it's not an entity. In fact, it can sanction persons and aircraft and vessels, but this is obviously not an aircraft or vessel.” So, they said, “First of all, it's not a person. You can't sanction it. Secondly, these smart contracts are not property. They're immutable. They're not owned. They can't be controlled.” And thirdly, they have a kind of last prong of their argument, even if this is property, even if there is an entity, the entity has no interest in this property. There's kind of a disconnect between the organization and the contracts because the contracts are immutable. They're just kind of operating out there in the Ether, no pun intended, but on the Ethereum blockchain.

So, this court, well, the district court throughout the plaintiff's case said, “No, OFAC's got broad authority to impose these types of sanctions. Tornado Cash is operated by an entity. A decentralized autonomous organization, has the characteristics that are typical of a variety of associations and organizations. It's an entity. The contracts are property. The DAO has an interest in the property because they earn fees from the use of this service.” So, no, OFAC acted and its authority. The plaintiffs appealed now to the Fifth Circuit, and the Fifth Circuit took a very different approach, a really, in many ways, unprecedented approach.

They applied the Loper Bright decision, which was, for many of you who know, a recent Supreme Court case that overturned the many decades of Chevron deference. The court said, even though we're not bound by OFAC's interpretation of this statute, IEEPA, we're going to look closely at it. OFAC's regulations say they're very broad. They say property includes contracts of any nature whatsoever, services of any nature whatsoever. OFAC said, “Come on, court, this is obvious. These are smart contracts. Our regulations say we can regulate contracts of any nature whatsoever.” But the court said, “No, not so fast.”

It was very clear in invoking Loper Bright, that the court was really uncomfortable with the very broad authority that OFAC has invoked under IEEPA, and the court did not defer to OFAC's interpretation, brushed aside the regulations and said, “Let's look at how smart contracts operate. Let's look at the definition of property,” and ultimately found that these smart contracts, because they're immutable, they can't be owned, they can't be controlled, they can't be changed. They're not property. They're not contracts. They're not services. So, they're outside of OFAC's regulatory authority and granted an order to remand and for the district court to grant the plaintiff's motion for summary judgment.

Ethan Ostroff:

Yes, Pete. A couple of things about that that struck me. I guess I don't know if you've thought about this, but the first was I was really surprised that I think what the court did was first it said, “Property is a plain meeting.” It goes through all these different dictionaries to get to the point of saying, "It has a plain meeting, but we need all these dictionaries to get there.” Capable of being owned. I think that's what it's sort of getting down to, is capable of being owned. Then said, “Well, look, an immutable smart contract like Tornado Cash is not capable of being owned because they operate without the ability of anyone to update, remove, or otherwise control the lines of code.” That immediately made me think of software being subject to copyright, and that software is considered, I mean, intangible property, right? I mean, that's sort of something that's

not really, hotly contested or debated, right? And can be owned, regardless of whether or not, like, for example, it's subject to an open source license.

So, I don't know. To me, that part of this kind of caught me off guard and made me think that is just a little strange. Then the other thing that caught me was the reference to contracts requiring two or more parties, but the court saying immutable smart contracts aren't really contracts because there's only one party. Is it put – there's only one party in play in the smart contract, right? I don't know, any thoughts about either of those points?

Pete Jeydel:

For sure. That's really the nub of the issue and you're not the only one who is surprised by the court's approach to this. OFAC is used to going into court and saying, "You don't need to look into it. You don't need to use dictionaries to find out what the definition of property is. Just look no further than our regulations. We'll be happy to help you out on this. Here's our regulations." They say, "We can do whatever we want. It's contracts of any nature whatsoever, services of any nature whatsoever." Look no further, court. Case closed. Thank you very much. But this court said, "No, we're going to pull out the dictionaries. We're going to question you, OFAC. This is a new Loper Bright world. We're not going to give you that traditional national security deference and Chevron deference."

It looks like a crazy result. You're right. The government's point was like, "Look, it's all bank. Can we not regulate banking software now? Can we not regulate automated banking transactions and financial transactions?" The court said that a service requires human effort. Here, this is a smart contract, it's operating in an automated manner. That's not a service because there's no human effort. The government says, "What? OFAC's been regulating the financial sector for many decades in ways that involve services where there's no human involved."

Ethan Ostroff:

It is shocking that after all these years of all this regulation by OFAC to think back that like property, such a central term like property is not actually defined in the underlying statute, right? I mean, that to me is just one of the – you sort of don't think about that, so it seems to me like one of the avenues here based on this decision for us potentially to see activity on the hill, a lot of the activity on the hill where there seems to be real bipartisan support is in the countering and the financing of terrorism, AML space. When you start talking about these things, you start to see, to me, people are more and more on both sides of the aisle interested in understanding the issues and making sure that we're doing everything we can, for example, to combat terrorism. And that includes like leveraging OFAC sanctions, right?

So, I'm interested in following this from that perspective to see if there's something done to update the statute in an effort to sort of address newer, more modern technologies, emerging technologies.

Pete Jeydel:

Yes. I mean, that's what the court said. The Fifth Circuit said, “Look, we don't like this outcome. We don't like the fact that based on our holding here, OFAC can't regulate these new technologies, but that's a problem for Congress to solve. We're not going to kind of gloss over the holes in OFAC's authority.” And Congress wrote this authority in a limited manner. It has to be property in order for OFAC to have the authority to regulate it.

Now, yes, I mean, the Trump administration is coming in and saying, “No more regulation by enforcement. We're going to be crypto-friendly,” but that made me in very different things in the kind of traditional domestic commercial financial context and the national security regulatory context, very different policy interests at play. I think OFAC would be very concerned about a statutory amendment to IEEPA. OFAC loves IEEPA just the way it is. They’ve been working very well in this world for many, many years. It's very broad, and that's traditionally the way OFAC has liked it because, again, OFAC can walk into court and say, “Don't worry about this. We know what this statute means. Here's what it means.” Case closed. Everybody go have lunch and have a nice day.

Ethan Ostroff:

So, with this, Matt, what are the sort of AML risks with mixers in general for developers, users, partners? What's that world look like now?

Matt Orso:

I mean, you see the obvious risks with the developers, which are playing out right now with the two Romans. Roman Storm and Roman Semenov and their criminal prosecution that's ongoing. You mentioned others though that are parties and potentially users of mixers. What type of risk, what type of exposure do you have simply for being an individual who decides to run some type of digital currency through a mixer?

At this point, there's nothing that says it's illegal. There are plenty of legal and non-illicit purposes, which I think Pete went over a little bit up before. One example I've seen recently is you have someone who is well-known because everything on a public blockchain is known to the world, somebody who holds significant crypto assets and then they become a target of some sort for others, for illicit activity, for potential crimes or whatever else, and they just don't want the world to know how much they have in crypto. That's not illegal to want privacy. That's another use that's legitimate of a mixer or a tumbler.

I'd say, it comes down to, for users, are you engaged in illegal activity or illicit activity or not? I think that's where your real exposure is, right? It's pretty traditional, but simply to use a mixer until there's a law, which there isn't, that I'm aware of, that says that it is illegal or against some type of regulation, I would think just a mere user should not have much exposure.

Now, when you talk about partners, which is another group that you mentioned, that could be another question. It depends on how closely are you involved in facilitating transactions, supporting some other aspect of a mixer. It depends on whether it's truly decentralized or not

and how closely you touch it. I can tell you that most national banks and large financial institutions are very hesitant to do business with or to bank something like this. A lot of it just is well above their risk tolerance and it just involves too much of a headache and impossible exposure from regulators from an AML perspective. But I think from that partner's perspective, it's a little more hazy and it's pretty fact-specific, I'd say, but you're still one level removed from the actual developers, right?

So, we're seeing it play out with the developers right now. Depending on where that goes, I think you could potentially see enforcement go in other places if the government's not successful, number one, or if they are successful and they want to take the next step. So, I really see the focus being on the developers right now and on financial institutions in the AML realm that they have their robust and compliant AML programs.

Pete Jeydel:

Why don't we talk for a minute about the actual criminal prosecutions against number one, Roman Storm and Roman Semenov, who were the two individuals who developed this protocol. I think it starts a little bit earlier though. They're not the first set of individuals to get charged with crypto mixing and crimes affiliated with that. In 2021, there was another Roman, Roman Sterlingov, who was a Swedish-Russian national. He was arrested in the US and charged for his role as the administrator Bitcoin Fog, which was a mixer where there was a large percentage of the cryptocurrency coming from the dark net market. This is narcotics, child pornography, human trafficking, et cetera.

So, this guy Sterlingov, he was convicted of money laundering, conspiracy to commit money laundering, and operating an unlicensed money transmitting business. He was just recently sentenced this past November to 12 years in prison. Similarly, you had someone named Larry Harmon, who was arrested in 2020, and he was the CEO of Coin Ninja, who operated Helix. This was also a darknet-based Bitcoin mixer, and so Harmon was charged with the same crimes that Sterlingov was charged with, money laundering conspiracy, unlicensed money transmitter, and he also was just sentenced this past November. He received only three years in prison, and this was on large part because he cooperated against Roman Sterlingov in the other case. He also had shut down Helix a couple of years before his arrest, so there were some unique factors there that led to a lesser sentence than the other.

With that said, you've got now these two individuals who developed Tornado Cash. The two Romans we'll say, Storm and Semenov. Semenov was still at large. He was never arrested by the government. News reports have him possibly in Dubai or somewhere else. The case against Roman Storm has proceeded though. He was arrested, is currently out on bail. Like those two prior prosecutions, they were charged with money laundering conspiracy, operating unlicensed money transmitter business. And here they also have another, an added charge, and what we've referred to IEEPA before, this is conspiracy to violate IEEPA. So, that's a unique aspect that didn't exist in the other two cases.

What the government alleges, alleges a lot of different things, but a big part of it is they alleged that Storm was aware that there were hundreds of millions of dollars in stolen crypto that was routed through Tornado Cash. They assert that Storm processed those funds through Tornado Cash's user interface and could have combated the laundering with his control of the user

interface. Another example, DOJ, they allege that Storm was aware that an OFAC-sanctioned wallet associated with the Lazarus Group out of North Korea that it was interacting with Tornado Cash, and while the government doesn't allege that Lazarus Group actually used the user interface for Tornado Cash, which Roman Storm allegedly controlled. The government says that Storm implemented a prevention measure in the UI that would be easy to evade.

Those are some aspects of the facts in terms of their theories of charging. Interestingly, on the conspiracy to operate an unlicensed money-transmitting business, on that charge, DOJ has argued that control is not a necessary element of a money-transmitting business, which is an argument that I don't believe we've seen before. They go back to the 2019 FinCEN Money Transmission Guidance for virtual currency, and they do a textual analysis and conclude that the term control is only one factor in a four-factor test for whether wallet providers are money transmitters, and so it's not essential. Control is not essential to being a money transmitter.

There are industry groups and others who, and certainly for Roman Storm and his lawyers, debate that position and say control is essential to being a money transmitter. We'll see how this pans out. The trial recently got pushed until April of 2025, and so we'll see how this all comes down in a number of months, but this will be an interesting one to watch.

Ethan Ostroff:

There's also this other case that's making its way through the Eleventh Circuit, I believe. Pete, what's going on with that case?

Pete Jeydel:

Yes. Again, just kind of stepping back, we are not at the end of the road here. We're kind of in the middle of this story, despite the significance of this Fifth Circuit decision, there's a lot of other things swirling. So again, there's the SDNY criminal case against Roman Storm, Roman Semenov, and there's a case that is now before the Eleventh Circuit, which is very similar to the Van Loon Fifth Circuit case. It's another group of Tornado Cash users that sued the Treasury Department in Florida, lost to the district court, like the Texas case that went to the Fifth, and now they're before the Eleventh Circuit, making similar arguments.

There are some distinctions. I think the government just put a brief in mid-December, following on from the late November Fifth Circuit decision in the Van Loon case, and the government said, “Yes, so we heard what the Fifth Circuit said about property, but first of all, they did challenge that head-on.” They said, “We think the Fifth Circuit's reasoning was flawed.” Again, this idea that there has to be human effort in order for something to be considered a service that, in fact, can regulate, they said that's absurd, as I discussed briefly before.

But really, they tried to recast the whole issue. Instead of focusing on these immutable smart contracts, the government's trying to recast it to focus on, “This is a service, and service is a type of property that OFAC can regulate.” Clearly, Tornado Cash, and the government argues, clearly Tornado Cash is providing a service. It doesn't depend on whether there's human effort involved. Similar issues, slightly new arguments, new court. We’ll see what the Eleventh Circuit says in the coming weeks, but I think that that's going to have a big impact on the government's strategy going forward. Is the government going to – is there going to be a circuit split? Is the

government going to appeal to the Supreme Court or take any number of other actions? Their strategy is still really up in the air, and I think they're waiting to see what the Eleventh Circuit does before they decide their next steps.

Matt Orsso:

The question is really whether possession and control are required elements of money transmission. Overall, I think it might just come down to what many white-collar prosecutions hinge upon, which is mens rea. For this case, did these individuals have an intent to promote the unlawful activity that occurred or not? I mean, this is a classic question for a jury and I think that that's what we'll get decided here in this trial in April.

One lesson from all these prosecutions stands out to me, which is that DOJ is most concerned with operators that intentionally conspire to launder the proceeds of criminal activity, whether that's the activity of transnational terrorist regimes in nation-states, whether it's site administrators on the dark net. If a crypto mixer is processing these transactions, especially if they're dealing closely with, Let's say dark site administrators, if they're mixing digital currency from those sites, I think they have a very meaningful risk of criminal prosecution.

I think we can talk a little bit about where we think the next administration might go, but let's first come back to what Pete was telling us about in terms of the Fifth Circuit and the Eleventh Circuit appeals, and especially, did those have any impact on the SDNY prosecution?

Pete Jeydel:

Well, certainly the Romans have argued that they do. So, they've filed some additional briefs with the court saying, “Look, Manhattan District Court, look at what just happened in New Orleans with the Fifth Circuit.” They've said, “You're prosecuting us for setting up Tornado Cash,” but the Fifth Circuit just said, “Tornado Cash is not property and no fact can't regulate it. So, let's go ahead and drop that conspiracy to violate IEEPA charge.” I don't think that the Tornado Cash decision can really play into their ML conspiracy and money transmission conspiracy charges, but on the sanctions violation conspiracy charge, they're saying, “Look, you can't prosecute us for this anymore because Tornado Cash is outside of OFAC's regulatory authority, according to the Fifth Circuit.”

I think that their argument has some merits, some weaknesses, as you were mentioning. The government alleged that the Romans had the ability to control Tornado Cash at least before it became immutable. That's my understanding. While it was a mutable smart contract, they had, according to the indictment, they had implemented some kind of compliance KYC measures after they became aware that the North Korean Lazarus Group was using the service. They, I think, blocked the Lazarus Group wallet. They may have made some kind of public statements about sanctions compliance, but I think there was evidence in the indictment about chats or something like that where they kind of said, “We know they're going to work around this.” And in fact, well, in the government alleges, this was all just window dressing. This was easy to circumvent, and they knew that. So, they were purposefully allowing the Lazarus Group and other SDNs and criminals to use the service.

From that perspective, the Fifth Circuit decision may not apply because, again, the Fifth Circuit decision turned on Tornado Cash is not property if it's unownable, uncontrollable, and unchangeable. But I think the developers of this code, they were obviously creating it, developing it, and changing this before the trusted setup ceremony after which the protocol became immutable. So, I think that the charges could still stick from the activity that predates that trusted setup ceremony while Tornado Cash was more clearly property and while it was mutable and changeable. So, I think the Romans are still pretty deep in it. I don't think this is going to be a get-out-of-jail-free card for them.

Matt Orso:

Yes. That makes a lot of sense, Pete. I'm thinking a bit about, "Can we read the tea leaves at all about what the go forward might be in terms of these types of enforcement actions, prosecutions, et cetera?" I think the answer is you can try, but you're never going to get it quite right until you actually see what happens. But from a DOJ perspective and from US Attorney's offices, I think it's always a comfortable place to be to charge the traditional frauds, whether it's wire fraud, whether it's conspiracy to commit money laundering. The kind of the core criminal financial crimes prosecutions. I think we'll continue to see that, certainly. The question is against whom and for what type of activity?

Will it continue to be certain types of mixers or people who facilitate mixing in some way if it's a decentralized protocol? I think the jury's out, but I would say I wouldn't be surprised, especially if you have a situation where individuals, there's some other facts that indicate there's an intent to transact with criminal actors, whether it's transnational criminal organizations, drug cartels, state actors who are sanctioned, the whole lot of them. I think the more that individuals are involved in either doing business with or setting up decentralized protocols that allow these types of offensive business, there's going to be criminal risk.

Pete Jeydel:

No question. I mean, to me, there's no doubt that, yes, I mean, from a USA's perspective, traditional fraud, these types of cases are easier to bring. But if you step on that third rail of a national security issue, if you have some indication that the Lazarus Group or North Korea or Russia or a terrorist group is involved in the picture somehow, there is no doubt in my mind that the Department of Justice is going to continue to bring IEEPA sanctions, export controls. Cases, the National Security Division has staffed up hugely in the last couple of years with, I think, 30 or so additional trial attorneys. They are going to keep bringing these cases. There's no doubt about that. They're going to fight this as well. The question is, how did they fight it? Are they going to – again, right now, they're focused on the Eleventh Circuit. Will they appeal to the Supreme Court? Will they litigate the scope of the remand order when it goes back to the district court?

I mean, I think there's a lot of lack of clarity about exactly what this Fifth Circuit order does here. Is the district court going to order OFAC to delist Tornado Cash? On the one hand, that's what the order on its face appears to call for, but the ruling, the reasoning was much narrower than that. Just said, "These immutable smart contracts are not property." The Fifth Circuit did not hold that Tornado Cash is not a person that cannot be sanctioned. In theory, Tornado Cash can potentially remain on the sanctions list, along with its website and wallet addresses and the like,

if it ever has property in the future, if they try to change the protocol or if they develop a new protocol, that would be potentially blocked property prior to a trusted setup ceremony, prior to it becoming immutable.

So, I think the government is not folding here. They're going to keep fighting this. This is right at the core of the government's national security regulatory authorities and priorities, and they're not going to let this go easily.

Ethan Ostroff:

I guess, guys, just to wrap up today, I was wondering, just to open the floor to both of you, I guess, number one, any additional thoughts about OFAC implications looking forward, particularly as to regulation of new technologies? And what, if anything, should traditional financial institutions make of this, be thinking about, or be considering?

Pete Jeydel:

This Fifth Circuit case went through a lot of, it's like 40 pages about how immutable smart contracts work, dictionary definitions, very technical, very detailed, but there's an element in the decision that is of much bigger potential significance, which is, will this be the beginning of a new trend of courts applying Loper Bright in the national security context? Is that going to be overturned? Is this going to be an aberration? Or are we going to start seeing It's questioning OFAC's interpretation of its statutory authority and not applying many, many decades of traditional national security deference to agencies like OFAC and federal prosecutors when they're bringing a sanctions case.

If Loper Brite is going to be the new norm in the national security context, that is going to make the government's life much, much more difficult. As new technologies emerge, they don't fit neatly into these decades' old statutory constructs. The government's going to have to fight much harder for each case rather than just again saying, "We've already defined this. We know exactly what this means. Defer to us." Case closed.

Ethan Ostroff:

So, that's one thing you're really looking forward to in that Eleventh Circuit case is to see which route that particular panel starts with?

Pete Jeydel:

Exactly. So, that's going to be a key thing to look out for, but I think at the end of the day, these issues are so important to the government, to the federal government, that whether it's through another act of Congress or more favorable litigation results, OFAC, DOJ, FinCEN, the rest of them will continue to enforce these laws aggressively, particularly, again, when you step into a national security issue like North Korea, terrorists, et cetera. So, if you're a traditional financial institution or a FinTech or others, do not take from this case, "Oh, we can let up on compliance. This is a new day for DeFi platforms, technologies." No, absolutely not. They should maintain their compliance approach. That means KYC, screening. There's all kinds of guidance from

OFAC, FinCEN, and others about what that compliance approach should look like. So, it's really important for traditional and new and emerging financial institutions, DeFi protocols, and the like to maintain their focus on compliance and not take the wrong messages from this decision.

Ethan Ostroff:

All right, Pete and Matt, thank you both for joining me today and talking about these very interesting issues Thanks to our audience for listening to today's episode of *The Crypto Exchange.* Don't forget to visit our blogs and subscribe so you can get the latest updates. Please also make sure to subscribe to this podcast via Apple Podcast, Google Play, Stitcher, or whatever other platform you may use. We look forward to our next episode.