Consumer Finance Monitor (Season 6, Episode 25) A Look at the Treasury Department's April 2023 Report on Decentralized Finance or "DeFi"

Speakers: Alan Kaplinsky, Peter Hardy, Lisa Lanham

Alan Kaplinsky:

Welcome to the award winning Consumer Finance Monitor podcast, where we explore important new developments in the world of consumer financial services and what they mean for your business, your customers, and the industry. This is a weekly podcast show brought to you by the Consumer Financial Services Group at the Ballard Spahr law firm. I'm your host, Alan Kaplinsky. I'm the former Practice Group Leader for 25 years, and now Senior Counsel of the Consumer Financial Services Group at Ballard Spahr. I'm very pleased to be moderating today's program. For those of you who want even more information, don't forget about our blog, consumerfinancemonitor.com.

We've hosted the blog since 2011, so there's a lot of relevant industry content there. We also regularly host webinars on subjects of interest to those in the industry. To subscribe to our blog, or to get on the list for our webinars, please visit us at ballardspahr.com. If you like our podcast, please let us know about it. Leave us a review on Apple Podcasts, Google, Spotify, or wherever you obtain your podcasts. Also, please let us know if you have ideas for other topics that we should consider covering, or speakers that we should consider as guests on our show.

Okay, let me tell everyone what we're going to be covering today. This is little bit different than our typical fare, but nevertheless, this is an extremely important subject. On April 6th of this year, the Department of the Treasury published the 2023 DeFi Illicit Finance Risk Assessment. This is the first Illicit Finance Risk Assessment conducted on Decentralized Finance, which is what DeFi stands for, in the world. This has never been done before. The assessment considers risks associated with what are commonly called DeFi services.

I can't think of two people more qualified to talk about this subject and to break it down. Really make it very easy for even those Luddites like me, who certainly are not very tech savvy. I know both of my colleagues at Ballard Spahr are going to do a great job today. First of all, let me introduce to you Peter Hardy. Peter is a partner in Ballard Spahr's Philadelphia office. He is the co-leader of Ballard Spahr's Anti-Money Laundering Team. He edits the firm's financial corruption blog, Money Laundering Watch. I was remiss, and I apologize to Peter for my introduction.

When I touted our Consumer Financial Services blog, I forgot to tout the excellent blog that you have, called Money Laundering Watch. Those of you that subscribe to the Consumer Finance Monitor, you should definitely subscribe to the blog that Peter manages. Peter also co-chairs the Practicing Law Institute's AML, or Anti-Money Laundering, conference each year. He serves on the Steering Committee of the Cambridge Forum on Sanctions and AML Compliance. Before entering private practice at Ballard Spahr, Peter served for 11 years as a federal prosecutor in the Eastern District of Pennsylvania. Peter, a very warm welcome to our podcast show.

Peter Hardy:

Thank you, Alan, and thanks for the shout-out on the blog.

Alan Kaplinsky:

Now, let me introduce my other colleague who's joining you today, Lisa Lanham. Lisa co-leads the firm's Fintech and Payments Solutions team. Her practice focuses on financial services matters related to the state licenses and federal approvals, that are necessary to conduct business for a variety of asset classes and market participants. Her clients include residential and commercial mortgage brokers, lenders, servicers, loan fulfillment providers; student, consumer, and solar loan lenders and servicers; entities offering retail installment contracts for the purchase of consumer goods; marketplace lenders; and investors who engage in secondary market activities related to all these business lines. She also works with early-stage FinTech companies in all these business lines to help develop products, being mindful of state licensing and regulatory compliance requirements. She helps those clients obtain and maintain any required state licenses and approvals necessary to engage in business. Lisa, a real pleasure to have you on our show today again.

Lisa Lanham:

Thank you, Alan.

Alan Kaplinsky:

Okay. We're now going to get into this subject, and we're going to break it down so our listeners understand it. Peter, first for you, could you give us... We're going to get an overview of this Treasury report I mentioned, and the recommendations that Treasury is making. First of all, can you discuss this sort of squishy definition of what decentralized finance is? My guess is, most of our listeners probably don't have a clue what that means. And how the definition will cause some issues in determining who the report and recommendations actually apply to.

Peter Hardy:

Sure, Alan. Thank you again for the introduction. Yeah. Let's talk about the definition. Also too, the report notes that it doesn't, of course it doesn't, alter any existing legal obligations, or issue any new regulations, clearly, or supposedly establish any new supervisor expectations. But it is fair to say that this document is going to be important in terms of all of those things, and how people think about DeFi. How does the report, to your question, define DeFi? Well, first it acknowledges that there is no generally accepted definition. But for the purposes of the report, what Treasury says, they define it as, quote, "Virtual asset protocols and services that purport," their word, purport, "to allow for some form of automated peer-to-peer transactions," end quote. That is their definition of DeFi.

However, the overall tone I think of the report is that it generally takes a rather dim view of DeFi, or at least some persons involved in DeFi. I'll get into that in just a minute. It starts off by stressing that, in the view of the government... And we have heard this before, speeches by regulars and whatnot... That even though DeFi kind of identifies itself, if you can even say it that way, as technology that's not really run by a human being, Treasury kind of disagrees with that. Remember, they're thinking about enforcement actions. The report stresses that DeFi services often do have a controlling organization or a person, that provides at least some measure of centralized administration and governance, including distribution and concentration of, for example, governance tokens and voting.

The report makes a point repeatedly that claims of, quote, "decentralization" are, in the view of Treasury, quote, "overstated," and they, quote, "vary in their accuracy." At times the use of that phrase reflects, quote, "marketing more than reality." I think what Treasury is saying, I'm simply repeating or channeling the views of Treasury, is that when some folks refer to a product or a service as decentralized, in their minds it's code for, we're not covered by the money transmission laws, for example, of the states or the federal government, the Bank Secrecy Act.

It also goes out of its way to critique industry critiques regarding a lack of regulatory clarity. Saying that actually, in the view of FinCEN or the SEC or the CFTC, they perceive their public statements, guidance and enforcement actions over the last 10 years as providing clarity. Now I'm just putting it out there. We're not going to get into that. That's a huge topic. Obviously, vast swaths of the industry would beg to differ. As we're recording this, the SEC just sued Coinbase and Binance, which are not DeFi. But I think it's fair to say that whether or not the SEC has or has not been clear in the past is a hotly contested issue, but it is nonetheless in the Treasury report. A few other things, and then I'll turn it over to Lisa here.

What's kind of at the heart of the report, the heart of the report finds that there's all sorts of bad actors. Ransomware, cyber criminals, scammers, actors in sanctioned countries, use DeFi services for the process of transferring and laundering illicit proceeds. They also find that criminals like DeFi for transferring illicit funds, because they don't have to provide customer identification information. Which makes it, in the view of Treasury, extremely appealing to criminals. There's all sorts of laundering techniques and transmission techniques involving obfuscation that can involve DeFi services, such as decentralized exchanges, cross-chain bridges, mixers... We'll talk a little bit about that at the end, some enforcement actions involving mixers... And liquidity pools.

After using all these techniques, criminals can then use centralized exchanges to exchange virtual assets for fiat currency. In the view of the government. It's kind of this perfect instrument for moving illicit funds, moving funds related to terrorism, and laundering money. The final thing is the report does observe that most DeFi services conduct transactions using smart contracts that are settled on the public blockchain, rather than through internal order books or ledgers, or private blockchain. Why is that important? It's often said or bandied about that crypto is anonymous or pseudo anonymous, but that it can be ultimately traced, because the ledger is public and it's immutable. That's not really true.

If you conduct transactions on a private blockchain, or on your own internal books or ledgers, it is functionally impossible or near impossible to trace. However, most of the transactions do occur on the public blockchain. But even as to that, Treasury ends on a bit of a dim note. It finds that there's significant limitations on relying on the public blockchain information to trace illicit funds. There's all sorts of businesses out there that assist the government in tracing funds and the government itself. This is what it says. I'm going to read a quote. I think it's actually important, because it just reflects, in the view of the government, just how difficult it is to actually trace illicit funds, particularly given constraints of time and money and personnel.

It says, "While regulators, law enforcement and public blockchain companies can in some cases identify transaction participants, they may in other cases only have their participants' wallet addresses without additional identifying information. Users can obfuscate the tracing of transactions in the public blockchain through the use of," here we go again, "mixers, cross-chain bridges, or anonymity enhanced cryptocurrencies, AECs." We see that phrase coming up in enforcement actions, which can create challenges for blockchain tracing. It goes on, but it has a rather pessimistic view as to the success rate or the possibility of a lot of these services that are out there. These are very good services, and they're attempting to make crypto finance safer for consumers and for the financial markets. But Treasury is at best skeptical about just how successful these are.

Alan Kaplinsky:

Okay. Lisa, you've got some points I know that you want to make.

Lisa Lanham:

Yeah. Peter and I get to work on a lot of these more interesting projects together. We see a lot of people coming through our practice groups, where they're tokenizing products or they're tokenizing something. I think that when I speak with state regulators, when I read reports like this, there's always this sort of angle that what we're talking about for DeFi is a cryptocurrency. That's just not always true. There's tokenized assets in all sorts of shapes and forms.

We've considered things like carbon credits, and fine art, NFTs, just things that are not a currency. It's not something necessarily that it's like one-to-one fiat currency, or crypto fiat, like a stablecoin. There's things out there that are just not, they're DeFi, but they're not money necessarily. It's an ownership right. I was just sort of curious. When I read this, Peter, I was thinking more like, what are the bounds on what DeFi could be, and how does this apply to something that's maybe not a crypto? I think that it's something that regulators have been struggling with for a long time. I know of a number of them that are coming out with, or have come out with, or plan to come out with these virtual currency business licenses, similar to what New York did with the New York BitLicense. They don't understand DeFi. They don't understand stablecoins. They don't understand NFTs. Technology is moving faster and tokenization is moving faster than regulators can. I think it's just always a gray area. You have to make your best judgment call as a business, as to what you do to protect yourself in this gray regulatory space.

Alan Kaplinsky:

For the Luddite that I am, Lisa, tell me, what is tokenization? What is that? Do you mean you can tokenize fine art? Tell me what that means.

Lisa Lanham:

Yeah. It's essentially like you're taking somebody's data or data about something, and you're turning it into something that's a symbol. You retain all the essential information about what the data is, without compromising its security. That digital token is your ownership right over physical or digital assets. Sometimes when I try to explain NFTs to people, it's like baseball trading cards, but it's digital. You're buying the trading card, and you're holding onto that trading card. The digital version of that sort of represents your ownership of it. There's people out there that are doing things that they're tokenizing things that are not money. You pay money for it, but it itself is not money. State regulators are struggling with that.

Alan Kaplinsky:

Why in the world would anybody want to buy some digital token that's somewhere out there on the internet or the blockchain? What's the point?

Lisa Lanham:

They can be insanely valuable. It's like having a Babe Ruth rookie card sometimes, and you can sell it for lots of money. They appreciate in value, some of them, based on their uniqueness, if we're talking about NFTs. There's reasons why people do it. The same reason why we all, like I said, bought baseball cards when we were kids.

Alan Kaplinsky:

Well I know, speaking for myself, if I want a piece of art, I want to hang it on my wall so I can look at it, and people come can come in and admire it. It makes me happy. Is there a happiness factor?

Lisa Lanham:

I mean, I can see it with my kids sometimes. They'll play these video games, and you buy sort of upgrades to your video games. There's interesting ways of doing it, in this sort of new generation, that it's interesting and exciting and cutting edge.

Alan Kaplinsky:

Okay. All right. Let's turn to another subject. I want to go back to Peter. Peter, what sort of impact do you think this is going to have on the industry, and where is the industry going with this?

Peter Hardy:

Yeah. The report does make several recommendations, as I mentioned. First of all, the report says... Although this is kind of, I mean I don't find this statement very helpful, because it's a truism and it doesn't really shed very much light. But they say that any DeFi service that functions as a financial institution, as defined by the Bank Secrecy Act, will be required to comply with BSA obligations. Of course that's true, on its face. But the question is, are you or are you not a, quote, "financial institution." This gets into the issue of whether or not DeFi is properly understood as being administered by a human being.

Treasury also emphasizes that any DeFi service that does business wholly or in part in the US, which includes accepting or transmitting virtual assets from one person to another by any means, then they're going to qualify as a money transmitter. A money transmitter or a money service business is covered by the Bank Secrecy Act. Then obviously, there's also state laws on which Lisa, not myself, is the expert. Despite this, though, the report goes on to say that there are certain DeFi's that purposefully seek to decentralize a virtual asset service, to try to avoid triggering AML obligations.

I think this gets back to the point about sometimes it's, in the eyes of Treasury, more of a marketing slogan than a legal or factual reality to say that you are DeFi. However, the report nonetheless does acknowledge that there are certain forms of decentralized activity that may not be covered by the Bank Secrecy Act. Without getting too much into the weeds here, it essentially references language that's contained in a 2019 publication by FinCEN that kind of covered the landscape, and it highlights Treasury. The report highlights what's called disintermediation activity, which basically is activity that involves unhosted wallets that retain custody and transfer the virtual assets without the involvement of a regulated financial institution.

One issue noted in the report, and this is getting back to my comment about the FinCEN 2019 publication, is whether activity is truly disintermediated. Throughout this is this kind of issue of, Treasury thinks that decentralization is often a phantom. It's not real in the real world. That there's always, or almost always, a human being who can be tagged who is in one way or another controlling or guiding whatever it is you're talking about. One legal issue as to whether or not activity is truly disintermediated, is whether or not an individual or an entity retains what's called an administrative key to the virtual assets, or a smart contract. And is able to, say, change a smart contract.

Then you get into issues, and this is the key word, at least for the legal analysis, of control. If there's control, says Treasury, then it's not really decentralized. It goes on a bit here. Essentially, this is one of the gaps that is cited in the report. Like I said, there are some recommendations. There's several of them, I'm going to focus just on two. They're all pretty high level. They're not very specific, and therefore not terribly helpful. One of them is assess possible enhancements to the US AML, countering the financing of terrorism regulatory regime, as applied to DeFi services.

Translated, amend the BSA so as to apply to DeFi. Now I'm not sure exactly how that would occur. I'm not talking about congressional fighting. I'm talking about, given the issues we've just discussed, I don't know what that law actually would look like, but maybe I haven't thought about it hard enough. I think it really kind of gets back to the fact issue, involving the laws that are already on the books. Okay, is this really just self-functioning, or is there actually a human who can be tagged with it? Then there's other recommendations regarding taking additional regulatory actions. I'll just end with this question on one final note.

Don't forget, regardless of whether or not the BSA applies, regardless of whether or not a state money transmitter law applies, or the security laws or whatever, Title 18, which is the federal criminal code, always applies to activity in the US. I'm talking here about the actual money laundering statutes, and also OFAC and sanctions, which is a key consideration in this field.

When I was talking before about how they say, "Sometimes these blockchain analytics really actually aren't that great at being able to trace certain activity," yeah, it's talking about money laundering. But a big thing there is sanctions and sanctions evasion.

Alan Kaplinsky:

Right. Hey, before we turn it back over to Lisa for her state law reaction, is there any mention made in the report of artificial intelligence? One of the main points or takeaways that I glean from what you said, Peter, is that the Treasury can always identify a human being that they can tag. If I understand machine learning or AI correctly, we may reach the point where there is no human being involved. Where the machine is actually in control, not a human being.

Peter Hardy:

Alan, that's a great question and a great point. I am 99% certain that the report does not mention AI.

Alan Kaplinsky:

Yeah, okay. That'll come out probably in a few years.

Peter Hardy:

That's next year. Yeah. It will be written by our robot masters.

Alan Kaplinsky:

Yeah, right. Correct.

Lisa Lanham:

Yeah. ChatGPT is going to write it.

Alan Kaplinsky:

Lisa, yes. Go ahead. State law.

Lisa Lanham:

I mean I've been hearing about crypto and all of this in the state law world for quite some time. But I'd be remiss not to point to the recent FTX collapse as a reinvigoration of all of the states to figure out how all of this fits into their regulatory schematic. I mean we're seeing states, like New York especially, they were one of the first states to come out with a license to regulate virtual currency activity. They're coming out with industry guidance about how it is that you're supposed to, custody assets and what your reserve should be. They're trying to make sure that everything is just more buttoned up.

Peter, I hadn't considered it. A lot of this, when we speak with these regulators, they are thinking about this like there's some human being at the helm with control. Oftentimes, it's not. It's algorithms, it's computers. There might be one person pressing a button, but that person doesn't need to have actual control over anything. Yeah. We're seeing industry guidance come out of New York DFS. Alan, you and I recently spoke with Kaitlin Asrow over at DFS about that on a podcast. More recently, New York's AG announced the Crypto Regulation, Protection, Transparency, and Oversight Act.

It proposes a lot of things to be regulated, like conflicts of interest and ownership in crypto issuers, marketplaces, brokers and investment advisors. There's public reporting of financial statements, and auditing requirements and standards, increased investor protection. The state's getting, now they want to codify something, not just put industry guidance out there from the state's primary regulator over the space. We know from speaking with Kaitlin that there's a number of states that New York is working with, to work on more stringent crypto regulation. They're working with the CFPB.

I just sort of think that what's happening in New York is indicative of what we're going to see throughout the rest of the country, as time goes on. I mean, honestly, we have our eyes on my corner of the world, on California next. Given DFPI's recent inquiries, and license suspensions for a couple of businesses after the FTX collapse. We also have our eyes on Illinois. They recently announced a landmark FinTech digital asset bill, which would establish really stringent regulations for digital asset businesses. Modernize the money transmission regulations to contemplate crypto, and it includes a licensing component like New York's BitLicense.

Alan Kaplinsky:

Okay. Peter, have we seen any actions by the federal government or state governments against crypto companies? We have mentioned already, well I think you mentioned what's going on with Coinbase and Binance. We've also referred to FTX, but what else is happening there? This seems like an area that is ripe for enforcement actions or litigation, with the industry guidance and reports being issued.

Peter Hardy:

Yeah. It certainly is ripe for enforcement action. Now Coinbase and Binance, I mean those are not decentralized. Those are very centralized. A lot of the difficulty in the enforcement from the government side is really on the investigative end. Nailing down, consistent with everything we've been talking about, exactly who or what is your target? I'm going to talk about two examples. I'm going to talk about ChipMixer, and then I'm going to talk about Tornado Cash. ChipMixer is, relatively speaking, a much more straightforward application of enforcement. Tornado Cash, for reasons that I'll chat about, is a lot more controversial and certainly much more interesting.

ChipMixer, in March of this year there was a coordinated effort with the FBI, and then Europol and the German police. This is reflective of really just the growing international organization and coordination, not only with crypto, but just with AML in general. It used to be that you'd never see stuff like that. Now you see it a lot, where law enforcement from different countries are working together. They shut down the dark net cryptocurrency mixing service that was called ChipMixer. They also got two court authorized, authorized by US courts, seizure of two domains that had directed users to the ChipMixer service. The German police seized about $46 million in crypto.

Meanwhile, right here in Philadelphia, the US Attorney's Office filed a criminal complaint against the alleged founder of ChipMixer. He's a Vietnamese national, Mr. Nguyen. And charged him with money laundering, operating an unlicensed money transmission service that's under the... Actually, that's not under the BSA. That's 18 USC 1960, although you become a money transmitter under the BSA... And also identity theft. Essentially what the criminal complaint alleges is that ChipMixer is a crypto mixing service. We already referenced the mixing, also known as a crypto tumbler. These are basically anonymity tools, that transform transactions of potentially identifiable or tainted crypto funds to others, which basically obfuscates the trail.

This gets back to the comment in the Treasury report, which makes it very difficult for law enforcement or anyone to trace these transactions. There's a lot of detail in the complaint. I'm not going to get into it. There's a lot of kind of salacious details, a lot of large numbers. Some stolen funds were tracked back to the Lazarus Group, which is a notorious hacking group that is based in North Korea. The complaint also alleges that ChipMixer processed cryptocurrency on behalf of our good friends in the Russian Military Intelligence Services, commonly known by their former acronym of GRU.

Definitely some bad actors here were enjoying the services of ChipMixer. ChipMixer, according to the allegations in the complaint, literally marketed itself as a tool for criminals. I mean, it was just out there. Mr. Nguyen apparently unwisely posted on a Bitcoin forum, among other things, quote, "If you want to hide who you are, ChipMixer is the perfect way." Perhaps not, but that's what he said.

Alan Kaplinsky:

Yeah, I wonder what lawyer gave him that advice.

Peter Hardy:

Yeah, not Ballard. Now let's turn to Tornado Cash. Tornado Cash is much more esoteric and more difficult. This really gets to the heart of what we've been talking about on the federal side. Tornado Cash is a virtual currency mixer that operates on the Ethereum blockchain. In August of last year, OFAC basically sanctioned it. What does that mean? According to OFAC... And I said it, not him or her... Tornado Cash receives a variety of transactions, mixes them together. In the press release by Treasury at the time, it said, "Despite public assurances otherwise, Tornado Cash has repeatedly failed to impose effective controls designed to stop it from laundering funds for malicious cyber actors on a regular basis, and without basic measures to address its risk."

Now the reason I quoted that language is because it implies, it implies that there's actual people at the heart of this service, although it doesn't explicitly say that. This was a unprecedented action, and it's been extremely controversial, and not surprisingly, really disliked by many elements of the so-called cryptoverse. It also reflects the enormous power of OFAC. At the end of the day, if DOJ can't get you, or a regulator, OFAC's reach is just very broad and very powerful. I think this action was... I don't know this, I'm speculating, but it was specifically done because of legal obstacles that might have stymied other agencies. Like FinCEN, talking about that 2019 guidance, is it decentralized, is it not? This may be ultimately, because the government actually agrees that there's no person in control of a powerful technology that has an easy application for malicious uses.

You don't always have to use it for malicious use. You could use it for anything. There's a civil complaint about this. But I think the thinking of the government is, technology is actually not neutral. And it's not okay to create something that can be used by really bad people to do really bad things, and then walk away and say, "Hey, you can't take any action, because there's no one there." That, in the eyes of the government, may be precisely the problem. It's like putting a bomb in the middle of the street, and then saying, "Eh." I mean, I'm obviously channeling here the views of the government, not shall we say of the crypto industry.

A final point on Tornado Cash, because this just really kind of brings it home. A civil complaint was filed against OFAC. You might ask yourself, by who? Normally, if you're sanctioned by OFAC, there is a process for a business or a person to petition OFAC and say, "You were wrong. Please take it back." One view of the argument is, there's literally no one to do that. It was a couple of plaintiffs who have assets that are basically now trapped through Tornado Cash. There's also a person, and this is important to a First Amendment claim that's in the complaint, who wanted to anonymously donate money to Ukraine to help

fight Russia. There's three claims, and there's one under the Administrative Procedures Act. Now, this is definitely a fine legal point, but I think it's worth getting into.

The authority that OFAC had to do this is under the International Emergency Economic Powers Act, which is often used in sanctions enforcement. What the plaintiffs do, is they cite this language from the Act. It's that, OFAC has been delegated the authority to regulate certain activities involving, quote, "Any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property subject to the jurisdiction of the United States." The claim by the plaintiffs, and this complaint is still out there, is that there's no property and there's no person. So OFAC actually lacked the legal authority to do what it did. That's an interesting argument, and it may indeed have legs. Even though all of this is very complicated and cutting edge and whatnot, that's a meat and potatoes statutory interpretation question.

The other claims are First Amendment. I'm not here to I guess opine, but that seems to be... I'm not sure that claim's going to go very far. This gets into the whole purpose of anti-money laundering, which is the financial system is actually not supposed to be anonymous. The government's not very interested in that, and honestly, I don't think the federal courts are going to be either. Then finally, there's a due process claim under the Fifth Amendment, arguing that three of the plaintiffs have their ether that's been trapped. Their property, they can't get it, and this has been an unlawful taking. It's generated a lot of interest in the industry. Folks have chimed in on this. It will be extremely interesting to see how it plays out, because this was indeed a very unique and unprecedented action, in which OFAC designated a technology.

Alan Kaplinsky:

Okay. Lisa, what about what's going on at the state level?

Lisa Lanham:

I think on the state level, there's a similar focus on BSA/AML compliance, cybersecurity and data privacy issues. I know just in dealing with applications across all industries, we're seeing a lot of scrutiny for those types of policies and procedures that a company has. They're really looking into it. Some of these regulators, New York in particular, have very sophisticated people working for them that go through your policies. They want to see independent auditing and testing. They really want to dot all their I's and cross all of their T's, trying to figure out whether or not your program protects their consumers enough. You see that in some of the more recent regulatory actions as well. Especially out of New York, we've got Coinbase, Robinhood and BitPay.

We know from speaking with Ms. Asrow earlier on, that Coinbase and the DFS's reaction to the lack of sufficient controls in their BSA/AML compliance program is what's driving a lot of the state's industry guidance on how it is that companies should operate. It's reading almost as like a cautionary tale and a roadmap for what you should make sure that you are doing, based on DFS's findings. Different area, California I mentioned earlier. Post-FTX, they have this reinvigoration of figuring out how crypto fits into its regulatory schematic. What licenses you need to have, what policies you need to have, what should be regulated and what's not regulated. They've been policing this space again since like late 2022. There's been a particular focus on enforcement for unregistered interest bearing cryptocurrency accounts.

I mean, you can get an account that's secured by your crypto wallet. If there's anything interest bearing on it, then California's been kind of scrutinizing all of that. Lastly, Illinois, we're keeping our eyes out for that. That FinTech and digital assets bill that we discussed earlier on, it's supported by their Consumer Financial Protection Bill, which gives the Illinois regulator broad authority to enforce the FinTech bill. It strengthens its authority and resources for existing consumer financial protection. I think we're going to see out of some of the bigger states, some New York like enforcement actions, just as they get their hands on what crypto regulation should be.

Alan Kaplinsky:

All right. We're getting drawn toward the end of our show for today. Before we close it out, I'd like to get final thoughts from both Peter, and from you, Lisa. Peter, you want to go first?

Peter Hardy:

Sure. Thanks, Alan. I think a few themes that have arisen on the fro end here. Which is the power of OFAC, the trickiness of determining whether or not, whatever it is, is truly decentralized or not. Quite honestly, I'm going to pick up on your question. It will be very interesting to see if AI has a role in this, perhaps it already does. To channel something that Lisa said, the technology is certainly outpacing the regulators, which is not terribly shocking.

Lisa Lanham:

Yeah. My larger point would just be, defend yourself. Set yourself up to have a really solid compliance program. I know sometimes clients are curious why it is that Peter, a white collar lawyer, is joining me on some licensing calls. The truth of the matter is that these risks are out there for your company, if you're playing in this kind of a space. If you've got policies and procedures that maybe you haven't looked at in quite some time. If you're either endeavoring to go into a regulated space, or if you are already regulated and you haven't been examined in a while, those policies and procedures for your BSA/AML compliance in particular, they're going to come up and they're going to get scrutinized. I would just say, if it's me, I'm reviewing those P&Ps. Making sure that I'm testing appropriately, that I have training records, that I have everything just buttoned up, so that I can just drop it on a regulator if they ask me.

Peter Hardy:

Yeah. If I may, Lisa, what you said is completely correct. Okay, maybe someone or something is decentralized, and so they don't have to have an AML policy. But if you are... And I think this is what you're saying, or in part, there's a lot in there. If you are yourself doing business with something that labels itself as decentralized, that will certainly impact your own AML policy. Obviously, it's higher risk.

Alan Kaplinsky:

Let me end with a rhetorical question. Lisa or Peter, either one or both of you can answer it. What role do you guys play? Do you actually get into the weeds here? Review the policies and procedures that people have, and help them draft them, if they don't have them?

Peter Hardy:

Yeah, for sure.

Lisa Lanham:

I was just going to say. You're the one that typically drafts and works on the policy piece of it, at the very least, with our clients. Sometimes procedures can get a little bit difficult, because you have to know what's accomplishable by the company, and what it can actually execute on every single day. But that policy piece for sure. I mean, we just had somebody email us the other day looking for some help.

Peter Hardy:

Yeah. I mean it's the predicate question of, are you a money transmitter or a money service business in the first instance? Then two, if you are, okay. We'll do your policies for you, and advise you on other risks. Three, even if you're not, or it's unclear that you are, you're still going to probably want some sort of compliance plan. Again, OFAC and Title 18 is still flowing around out there.

Alan Kaplinsky:

Right, right, right. Well let me, first of all, thank both of you for enlightening our audience today, and enlightening me. I may have graduated, so I'm no longer a Luddite. I'm not sure what the next stage is, but I'm certainly not an expert close to the two of you. Thank you, again.

Lisa Lanham:

Thank you.

Peter Hardy:

Thank you, Alan.

Alan Kaplinsky:

Okay. To make sure that you don't miss any of our future episodes, subscribe to our show on your favorite podcast platform, be it Apple Podcasts, Google, Spotify, or wherever you obtain your podcasts. Don't forget to check out our blog, actually two blogs here, the consumerfinancemonitor.com blog, and the Money Laundering Watch blog. There is a lot of information, particularly on the Money Laundering Watch blog, but also on our Consumer Finance Monitor blog about the topics that we are talking about today. If you have any questions or suggestions for our show, please email us at podcast, that's singular, podcast@ballardspahr.com. Stay tuned each Thursday for a new episode of our show. Thank you all for listening, and have a good day.