Consumer Finance Monitor (Season 5, Episode 9): The Business of Cryptocurrency: A Discussion of Key Regulatory Issues

Speakers: Alan Kaplinsky, Mike Robotti, Peter Hardy and Marjorie Peerce

Alan Kaplinsky:

Welcome to Consumer Finance Monitor podcast, where we explore important developments in the world of consumer finance. I'm Alan Kaplinsky, Senior Counsel at Ballard Spahr and the former chair of the consumer financial services practice group at Ballard Spahr. And today I'm very pleased that we're going to be releasing on our Consumer Finance Monitor podcast a previously released podcast that was done by Ballard Spahr's Business Better podcast, which is separate and distinct from the Consumer Finance Monitor podcast.

Alan Kaplinsky:

But I thought that this was especially relevant to the listeners of our podcast. And let me tell you now what we are going to cover this afternoon. So this particular podcast features a very full discussion of cryptocurrency. What is cryptocurrency, and what are the rules that apply to this increasingly popular but complicated financial instrument? For those seeking to be in the business of exchanging crypto, what registrations and compliance programs are needed to meet regulatory requirements? And how should crypto exchangers and other financial institutions address crypto transactions involving unhosted digital wallets or requirements that counterparties in certain crypto transactions be identified and reported?

Alan Kaplinsky:

Our Ballard team today, who I will introduce to you in a moment, will help answer these complex questions and explain why it's very important to seek counsel before transacting any business related to cryptocurrency. Let me now introduce our speakers today. They are all from Ballard's white collar and internal investigations practice group. And moderating the conference today will be Mike Robotti and our presenters today are going to be Peter Hardy and Margie Peerce. All of them as I said are in our white collar and internal investigations practice group, but all of them are very active participants in our consumer financial services group because cryptocurrency is a type of consumer financial services. So without further ado, let me turn the program over to Mike.

Mike Robotti:

Thank you, Peter Hardy and Margie Peerce for joining me today. Before we get started, can you tell our listeners where they can find more information once they finish listening to today's discussion.

Peter Hardy:

Thanks, Mike. Happy to chat about that. And I just want to say thank you to everyone who has tuned in to listen to our podcast. So I can never resist giving a shout out to our blog, Money Laundering Watch. If you're interested in these issues, we certainly cover crypto. We cover all things money laundering and anti-money laundering. Please check out Money Laundering Watch, Ballard Spahr's blog. I'm a little biased, but it's a really good blog. And if you're interested in these issues, I think you'll find it useful.

Margie Peerce:

And I can ditto that it's a really great blog that Peter started. But what I want to just say is at Ballard, about four years ago, several of us recognized that crypto and blockchain were going to be very important areas that were going to require legal services. And so we formed a crypto blockchain group. And we have lawyers from almost every discipline in the firm who are

part of our group, intellectual property, consumer financial services, white-collar criminal defense, securities. You name it, we've got it. Corporate work. NFTs are now out there. I'm sure we're going to start having clients that want to do something in the metaverse. And so we offer you one- stop shopping for work on your crypto matters.

Mike Robotti:

So Peter, why don't you kick off our discussion here today? What are some of the US regulatory challenges facing cryptocurrency exchanges? In particular, what are the Bank Secrecy Act and anti-money laundering concerns?

Peter Hardy:

So there's a couple of parts to that question, and I guess I'm just going to start off very high level at first and keep it very brief. So the basics are if you're a crypto exchange, then chances are that FinCEN, Financial Crimes Enforcement Network, which is the regulator for the Bank Secrecy Act, is going to regard you as either a "exchange or an administrator." And the translation is what that means is that you are most likely going to be a money services business and therefore covered by the Bank Secrecy Act and/or a money transmitter under various state laws.

Peter Hardy:

I'll get to the state laws in a second. So what does that mean? Well, what it means is that you have to register as a MSB, money services business, with FinCEN. That's relatively easy, but it also means that then because you're covered by the BSA, you've got to have an actual anti-money laundering program and all that that entails; a compliance officer, independent testing, training, customer due diligence, et cetera, et cetera. So it's the day-to-day onus that can be difficult under the BSA in terms of running a functional program.

Peter Hardy:

Now under the states, the state's kind of a patchwork quilt, and in many states if you are an exchanger or an administrator, you do have to then obtain a money transmitter license and that has its own set of obligations and regulations. Other states, they take the position that crypto doesn't count as money or funds or whatever the magic word is under their state statute.

Peter Hardy:

So those are the basics. Now, in practice, and I'll use an example just to kind of illustrate it, typically the enforcement cases, whether criminal or regulatory under the Bank Secrecy Act have all kind of centered around a failure or an alleged failure to register properly as an MSB or a money transmitter.

Peter Hardy:

Now, the Department of Justice charged some individual executives at an exchange, very large exchange called BitMEX. And one of the interesting things about that prosecution is it actually wasn't based on a failure to register as an MSB, so it is a exception to the kind of general rule that I just noted, rather as a little more esoteric and they were considered by the government, BitMEX here, to be a financial institution covered by the Bank Secrecy Act because they were future commission merchants, which is a little unusual. But regardless, that was the position of the government. And those prosecutions are still pending. The gentlemen are, as of now at least, going to trial. And the allegation there was, is that they utterly failed to maintain the AML program that I just described. They're based in Seychelles Island.

Peter Hardy:

And there's another facet to that case that really is a constant theme. And a lot of the enforcement actions that we see, which is a exchange or a business that is, according to the government, not properly registered in the United States, supposedly operating abroad only, but they have US customers, which of course in the crypto world is very easy to happen. And so that's the jurisdictional hook and also part of the allegations, regulatory violations and criminality.

Peter Hardy:

And then just to follow up on that, FinCEN along with the CFTC settled a regulatory enforcement action with BitMEX itself, the organization versus the gentlemen who had been prosecuted, and the outcome of that was $100 million fine and a commitment to file suspicious activity reports that had not yet been filed. You have to hire an independent consultant who then needs to help them ensure that in fact they don't have any US customers. And what happened there is something that happens with regularity is that the US customers were using something called a VPN, which is a virtual private network, which then masks or usually masks your location. And the government allegation is that nonetheless BitMEX still knew that the folks they were dealing with included US citizens.

Peter Hardy:

So that's kind of a very high-level description of some kind of the core regulatory and criminal risks that folks can face if you're an exchange. And I want to just switch gears slightly and then kind of move on to some more pure regulatory things that have gone on lately. You know, let's say that you have your functional AML program and you're properly licensed in the US and you're doing everything you should, there's a couple of things coming down the pike that you still need to be aware of that could definitely affect you in terms of compliance costs and efforts of that nature.

Peter Hardy:

So one, to be a master of the obvious, the government's very interested in crypto right now. On the AML front, there's a big new law that was passed earlier this year, the Anti-Money Laundering Act. So it defines a money transmitter subject to the BSA as a business engaged in the exchange or transmission of value that substitutes for currency i.e., crypto. This pretty much just formalizes the longstanding position of FinCEN that I already described. So that's one.

Peter Hardy:

The other thing is FinCEN came out as required by Congress this year with a list of anti-money laundering national priorities. Crypto itself was not included in the list of eight priorities, but it definitely got a shout out. And according to FinCEN, it's the "currency of preference in a wide variety of online enlisted activities." And on that note, FinCEN this year created for the first time the position of Chief Digital Currency Advisor. So the point here is there's a lot of things that are converging and the government is definitely taking a coordinated or semi- coordinated approach to regulation.

Peter Hardy:

There's two possible regulations out there that I think are worthy of noting, and this will also apply to banks and other financial institutions as well. So FinCEN proposed a new rule for a "unhosted virtual currency wallet." So an unhosted wallet is one that's not provided by a financial institution or other service and it basically resides on a user's personal device or offline. So for transactions involving an unhosted wallet, and this kind of gets into a lot of the unique practical problems that crypto can pose for financial institutions, whether they be exchanges or otherwise, who are trying to comply with these rules because AML is all about transparency and identifying the true identity of your customer. So for a transaction greater than $10,000, the proposed rule, and it's still proposed, it hasn't been passed, would require banks and money services businesses to submit a report to FinCEN, analogous to existing reports for currency like a CTR.

Peter Hardy:

And so you'd have to have the full name and physical address of the client. The name and physical address, and this can get tricky, it's a practical matter of each counterparty to the transaction, the amount and type of virtual currency being transacted, the assessed value, and all other information that basically uniquely identifies the transaction, the accounts, and the parties involved. And it's really the requirement for the counterparty that gets very tricky because, and this bleeds into the second proposal that I wanted to talk about. Again, FinCEN proposed that the travel rule, which is an existing rule under the Bank Secrecy Act that already applies to banks, be greatly expanded.

Peter Hardy:

Travel rule essentially, to dumb it down, the information travels with the transaction. So again, if you are a financial institution that is on the originating side of a transaction, you need to know who is the counterparty, who's on the recipient side. So it would expand the travel rule to reduce the current $3,000 threshold to only $250 for international transfers, thereby greatly expanding it. And importantly, it would explicitly apply to transactions involving virtual currencies.

Peter Hardy:

So this is a bit of a challenge largely because of technology. I mean, the technology is being worked out, but unlike for traditional fiat transactions, there's no SWIFT system in place. SWIFT is the system that financial institutions use around the world to track counterparties and things of that nature. It just, there is no system in place for crypto. It's a particular problem if you're talking about defi or decentralized finance where, government may not agree with this, but there's no one there. There's no one running the system.

Peter Hardy:

Having said all that, the Financial Action Task Force, which is a anti-money laundering body based in Europe that provides standards for participating countries around the world, has long had the travel rule in place for virtual currency transactions over $1,000. So they're already there, although they actually concede that there's no technically proven means of identifying a virtual currency provider that manages beneficiary wallets. So they concede that, but they plunge ahead anyway.

Peter Hardy:

And the OCC is examining banks for the travel rule, the IRS is examining crypto exchanges for the travel rule and other requirements. So it's out there. And just to bring it home and then I'll stop talking, the BitMEX enforcement action that I referenced, the one that was recently resolved, had some language in there expressing FinCEN's expectation as a practical matter as to how virtual currency exchanges can indeed through various means, not necessarily easy, but they can find out information about past transactions and counterparties by using various address clustering tools.

Peter Hardy:

So that's a long-winded way of answering your question, Mike. The upshot is we've got the basics, the core BSA requirements, government is definitely active in this area. And beyond just the basics, there's some more onerous and more esoteric regulations that are potentially down the pike.

Mike Robotti:

So just to follow up on that, what about the US criminal money laundering statutes? What are the particular concerns there?

Peter Hardy:

Yeah. So let's not forget of the constant existence of the criminal code. And so that's Title 18 and here it's Sections 1956 and 1957. Those are the good old- fashioned standard money laundering statutes. And anyone who is going to be involved in crypto on the business side and frankly fiat currency, needs always remember regardless of FinCEN and the SEC and the regulators, there's always the prosecutors and the possibility that if you know, that's the key, if you have the mental state to know that a transaction involves so-called dirty money, then without getting into all the other elements of the statute, you could definitely be assisting or conducting a money laundering transaction, and especially with some of the practical problems of determining who you're dealing with.

Peter Hardy:

And it also always gets down to the constant question in AML and money laundering in general, which is source of funds, it always behooves folks to remember beyond just regulatory requirements, there is just that, and this applies to everyone, don't have to be covered by the BSA, you can be a real estate agent or whoever, you always got to worry about the Title 18.

Peter Hardy:

And when things first started, that's what the government was using. When you think about Silk Road prosecution, which was essentially an alleged drug, gunm and child porn bizarre. I mean, they charged drug charges and they charged money laundering. The industry obviously has greatly matured. I mean, there's still some bad folks out there, but obviously virtual currency is light years from those days. And so now we're really seeing more regulatory action.

Peter Hardy:

But again, the criminal code is always there. And there's, there's kind of an armchair debate about is fiat currency worse or is crypto worse in terms of the amount of dirty money or dirty funds that's being transacted. It's hard to say. And part of it depends on whether or not you're talking about investment transactions or transactions to acquire, what have you. There's a lot of folks that say that fiat is still the method of choice for money launders. And in terms of just raw numbers, that's probably true. But again, issues with knowing who the counterparty is and source of funds, yeah it's a particular issue for crypto.

Mike Robotti:

So let's focus for a minute on traditional financial institutions. What should they be thinking about if they are considering doing business with crypto?

Peter Hardy:

Yeah. So I guess it depends on the customer. I mean, if you're thinking about dealing with an exchange, because at the end of the day these exchanges need access, or many of them, to and desire access to the traditional banking system. Is your exchange properly licensed? Again, the state money transmitter laws can can be difficult because they're just all over the place and there's a lot of vagueness. And what are their own AML processes like? You know, that's part of your... So if I'm a bank thinking about banking a crypto exchange, and many banks really don't want to do it, but there's some out there who are willing to kind of take that on those extra compliance costs, you need to dig into the functionality of their own AML processes.

Peter Hardy:

If you're talking about individual customers, make sure that they're actually not functioning as a money transmitter. You know, maybe they are. Even if it's just a person, they could still be a "exchanger or administrator." And again, we get to the source of funds issue.

Peter Hardy:

I just want to wrap up. I think the really interesting thing now is traditional financial institutions that are themselves thinking about getting into crypto and the blockchain. And again, we get back to the regulators and there's been a lot of move, well sort of movement on this recently. So the FDIC earlier in 2021 sent out a request for information on the role of banks and crypto, and those responses came in over the summer. And then partly based on that, but some other activity as well, the FDIC along with the Federal Reserve and the Office of the Comptroller Currency issued in November a short joint statement on crypto asset policy. And they purported to produce a roadmap.

Peter Hardy:

Short story short, the policy statement itself really provides no concrete details. It really says in 2022 more clarity is forthcoming, which obviously would be very appreciated. The roadmap has five bullet points and these are the activities that the federal regulators are going to supposedly provide more clarity on in 2022 for banks that are thinking about getting into this.

Peter Hardy:

And a lot of this is, there's an AML component, but a lot of this is just kind of straight up bank permissibility issues. So crypto asset safekeeping, ancillary custody services, facilitation of customer purchases and sales of crypto assets, issuance and distribution of stable coins, and the holding of crypto assets on a balance sheet. So these are all things that banks are thinking about or starting to get into. And obviously, the regulators are taking a, shall we say, cautious approach. They call it a sprint. I'm not sure that industry would agree with the use of the word sprint.

Peter Hardy:

And then about the same time that this joint statement was issued, the OCC issued an interpretive letter, Letter 1179. And the upshot of 1179 is that on one hand, it validated and confirmed some prior interpretive letters by the OCC, which basically said the following. If you're a bank and if we examine you, the following activities are not categorically impermissible so long as you have sufficient processes in place. They covered a lot of the activities that I just ticked off that were on the roadmap. So as whether or not you can provide crypto currency custody services, this was Interpretive Letter 1170. So the more recent letter confirmed that.

Peter Hardy:

And there was also whether or not you can hold dollar deposits serving as reserves, backing stable coins. That was Letter 1172. So the more recent letter confirmed that too. And then finally, we've got letter 1174, which addressed whether banks can act as nodes. So we're really starting to kind of get out there on the blockchain, independent node verification network, and whether or not banks can engage in stable coin activities.

Peter Hardy:

So the upshot is that in this more recent letter, the OCC on one hand confirmed those letters. However, if you're going to do that, you need to get prior approval from your supervisory office, which on one hand makes sense, but it also suggests that the effect of this is that on one hand the OCC said we're not saying you can never do it, you just need prior approval.

Peter Hardy:

I think it's fair to say that obtaining the prior approval will be a rigorous and demanding process. And remember, it's only the OCC that's issued this letter. The FDIC didn't do it. The Federal Reserve didn't do it. So they still haven't gone on record about these things. And it's also fair to surmise that until that supposed extra clarity comes out, according to the roadmap, a lot of the regulators are probably going to hold back on opining on anything or offering their non-objection to requests to proceed with these activities.

Peter Hardy:

So it's a step forward, but we can also anticipate some continued delay in terms of clarity while the regulators continue their "sprint." But it's really interesting to see the traditional banks wanting to get into crypto and blockchain because obviously it's here to stay and everyone including the government acknowledges that.

Mike Robotti:

So Margie, why don't you jump in with your thoughts here? What types of criminal cases are you seeing regulators and prosecutors bring?

Margie Peerce:

Sure, thanks. And Peter, thank you very much for that. I think that what we can see just based on what Peter has said is this is a very complicated area. And you have overlapping regulators. You have regulators sometimes giving inconsistent guidance. As an example, the SEC has found that Bitcoin and Ethereum are not securities, but the CFTC has found that Bitcoin and Ethereum are commodities. So there's just a lot of confusion and complicated analyses that need to be done.

Margie Peerce:

So Peter's talked about money laundering and using Title 18 for money laundering. But what I'm seeing is a lot of crypto prosecutions brought under garden- variety mail and wire fraud prosecutions, as well as securities fraud prosecutions. And so what are mail and wire fraud? Mail and wire fraud are very simple. It's use of the mail or the wires to defraud another by using false promises or misrepresentation.

Margie Peerce:

So all that has to happen is the mail or a wire, and that could include UPS, it include FedEx, it can include any of these common carriers so long as there's some sort of "interstate commerce." So if there is a view that there were false statements made in the marketing or sale of a crypto product, then the US Attorney's Office, the Department of Justice, like you've been reading a lot lately, can bring a criminal prosecution, and they are doing that. And they are bringing criminal prosecutions for what we would call in the white-collar space garden-variety criminal conduct.

Margie Peerce:

And then you also have securities fraud charges, criminal securities fraud charges which are brought, as well as civil securities fraud charges. So what's criminal securities fraud or civil securities fraud? It's fraud in connection with the purchase or sale of securities. And you could have a civil charge for the unregistered sale of securities. You could have criminal charges if there's fraud in connection with that.

Margie Peerce:

And so what's a security? The SEC has come out with a complicated test, which is called the Howey test, which goes back to a Supreme Court case from the 1940s, which talks about an analysis that needs to be done as to whether a particular product constitutes a security. The commissioners of the SEC have basically said that they have not seen an initial coin offering, which is the equivalent of an initial public offering, they have not seen an initial coin offering which isn't offering the sale of a security.

Margie Peerce:

So basically, unless a particular token is considered to be a utility token, which means there's no profit to be derived from it, and don't just take this as the sole analysis because lawyers really need to dig into these things, before somebody engages in such a transaction. But if they conclude that something is not simply a utility token, there is a risk of civil actions taken by the SEC. And if they believe there was some fraud or misrepresentation in that sale, then you could find yourself as the subject of a criminal prosecution for securities fraud.

Margie Peerce:

So my most significant takeaway from all of this is that just because it is this digital currency, just because it's not something that you can hold, does not mean that criminal and civil regulators are not going to take a look at what one is doing. So the absolute best takeaway that I hope somebody can take from this podcast, and I so enjoy joining my partners, Mike and Peter, on this podcast, I hope the best takeaway you can all take from this is this is complicated stuff. This is complicated stuff. And as lawyers, we much prefer to be giving the advice at the front end of a transaction, at the front end of somebody embarking on a crypto business, then having to help them unwind what they may have done or defend them in regulatory scrutiny on the transactions they've engaged in.

Margie Peerce:

So if there's one takeaway from this, please go to an accountant and go to an attorney that can help you make sure that what you are contemplating doing is set up lawfully and properly.

Alan Kaplinsky:

Well I want to thank our participants in the podcast today, Mike Robotti, Peter Hardy, and Margie Peerce, from the white collar and internal investigations practice group. We discussed the business of cryptocurrency and this was a podcast previously released as part of Ballard Spahr's Business Better podcast. And I finally want to thank all of our loyal listeners today for taking the time to download our podcast and to listen to it. I hope you enjoyed it and I hope you have a very good rest of your day