The Crypto Exchange: Navigating the Dark Side of Crypto: Crime, Compliance, and Consumer Protection
Host: Ethan Ostroff
Guests: Michael Lowe and Brett Broczkowski

Ethan Ostroff:

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

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

Today I'm joined by my colleagues, Brett Broczkowski and Mike Lowe to discuss the intersection of crime and cryptocurrency, including some of the guidance available for financial institutions tasked with navigating this space. Brett and Mike, thank you guys for joining me today.

Michael Lowe:

Thanks for having me.

Ethan Ostroff:

Yes, of course. I thought we might discuss, start off with just a little bit of a high-level discussion. There's a lot that we hear about the intersection of various criminal actors and cryptocurrency. Is this something that really is a big deal or is it being overstated?

Michael Lowe:

I think it is a big deal, and in fact, I don't think it's being overstated at all. If you look at the data from the Internet Crime Complaint Center or IC3, which for those who are not aware of it, it's basically a website to the FBI runs that tracks and on which you can report Internet and various computer-type crimes. IC3 data is that for 2023, there were reported losses of over $5.6 billion, with a B, as a result of crypto-related crime. To put that into perspective as to what type of an increase that was over the previous year, that was a $2 billion increase over 2022's numbers, which were themselves an increase over numbers.

So, every year, crypto-related crime just keeps getting more and more serious, more and more prevalent. Also, you need to keep in mind that these are just the reported figures. I mean, the FBI can only track what people report, and the likelihood is that it's much greater than that.

Brett Broczkowski:

Exactly, Mike. We're also seeing trends that suggest the population most impacted by these crypto-related crimes are those over the age of 60. So, we're taking that figure, that $5.6 billion in losses reported in 2023, over $1.65 billion or nearly 30 % were attributable to that age category alone.

Ethan Ostroff:

To put this in context, right, when we talk about IC3 data points like this, this is consumer losses, right? We're not talking about institutional losses or losses by businesses.

Is that right?

Michael Lowe:

Well, no. I mean, we're talking about losses that are reported. So, it depends on who the victim here is. If an institution is a victim and they report it, it would get tracked on the website.

Ethan Ostroff:

Okay. So, this encompasses both sort of institutional and consumer or retail customers, right?

Michael Lowe:

As Brett pointed out, about 100 % of the victims of crypto-related crime are older people. So, most of what you're seeing here and most of what's getting reported is the individuals who find themselves defrauded in one way, shape, or form, and it has something to do with crypto.

Ethan Ostroff:

Brett, that data point you mentioned about nearly 30% being those over the age of 60s is interesting, I think, because we see significantly more activity by federal regulators, including the FTC and the CAPB, specifically about trying to prevent senior citizens and elder Americans from being duped by various different types of scams, which also involves crypto-related scams, but a larger focus by those federal regulators, specifically on preventing elder abuse and a wide variety of different products and industries. How have the various criminal-related agencies responded to this? Is there more criminal enforcement going on? Or has it remained the same?

Michael Lowe:

Ethan, you're right. There actually is more enforcement going on now, and it really started ramping up in about March of 2022 after President Biden signed an executive order that made clear that there was a need for coordinated enforcement as well as crypto market regulation. We can talk about those two things separately because they're different and the market regulation is a very controversial component of what this administration is trying to do.

But the point is that the administration did recognize that there was a need for coordinated enforcement. As a result, both the SEC as well as the Department of Justice have ramped up their enforcement efforts relating to crypto. So, for example, in May of 2022, the SEC nearly doubled its crypto asset and cyber unit. In September of 2022, DOJ established, essentially, a task force, which is really a network of over 150 federal prosecutors who were tasked with the role of investigating a prosecuting crypto-related crime.

In fact, I was just leaving DOJ when that effort was getting underway, and as it was ramping up, there was outreach seeking participation in that, that crypto cyber units, and that was something that I was asked to participate in, but because I knew I was going to be leaving, I didn't.

Ethan Ostroff:

It is an interesting another data point that the federal government is using a greater and greater percentage of its budget specifically for both regulatory and criminal enforcement matters, right?

Michael Lowe:

Yes.

Ethan Ostroff:

Let's talk a little bit about the intersection more specifically of cryptocurrency and criminal enterprises. What types of crypto crime are we seeing most frequently?

Michael Lowe:

So, Ethan, I would say there's really four primary ways in which crypto is being utilized to further criminal activity. It's really, for a long time now, been the preferred payment method. For a long time now, it's been the preferred payment method for criminal activity because of its difficulty of tracing crypto.

Second, crypto has become widely used in various scams, particularly because it's not well understood. I mean, you talk to people about crypto and there are a lot of people – I'd say the majority of the population really doesn't understand crypto. Third, you have the DOJ and SEC have been prosecuting or suing various types of crypto-related investment fraud. And then finally, you have the prevalence of money laundering which currently is done using crypto mixers, which have dramatically increased the scale of the money laundering involving crypto.

Ethan Ostroff:

Okay, so maybe we could talk about sort of those one at a time. The first one being a preferred method of payment for illicit activities. Can you talk a little bit about how that's developed over the last decade or so, 15 years?

Michael Lowe:

Crypto and primarily, Bitcoin has been a preferred payment method for illicit activities, basically, since its inception. Within two years after the birth of Bitcoin in January of 2009, there was a black market known as the Silk Road, which had opened on the dark net. That market dealt

primarily in narcotics. It accepted payment for transactions exclusively in Bitcoin. Even though it only operated for about two years before it was shut down, the Silk Road processed over 9,519,000 Bitcoin, which for anyone who knows what Bitcoin costs or worth today, that's over in today's dollars $577 billion, with a B.

So, in two years, Silk Road processed today's equivalent of $577 billion in Bitcoin used to purchase or facilitate illegal conduct. That particular website, the Silk Road, was seized by the FBI and its founder, a guy named Ross William Ulbricht, who operated the site under the pseudonym, the Dread Pirate Roberts, for those listeners familiar with Princess Bride. Ulbricht was sentenced to double life in prison without the possibility of parole. Interestingly, as an aside at his sentencing, the judge found by a preponderance of the evidence that he had actually not only done these things involving the Silk Road, but he'd conspired to engage in murder for hire. He apparently paid over $700,000 to hit men to kill five people who were threatening to reveal or disclose the Silk Road in his enterprise. That fact was considered by the judge in imposing that double life sentence. Now, thankfully, nobody was killed, but he did, apparently, try to kill people.

Ethan Ostroff:

Interesting. So, in the context of the payments use case you were referring to. One of the big issues there is traceability and questions revolving around anonymity. What I would describe as anonymity versus pseudonymity. In other words, can the federal government really trace all these transactions on a blockchain to show the movement ultimately between person one in person two, even though it may be moving through numerous different wallets and potentially even one or two mixers in there between?

Brett Broczkowski:

Yes. So, Bitcoin's blockchain is indeed public. When you have cooperation between legitimate exchanges such as Coinbase and federal agencies, that's when you get these takedowns, right? Now, when you add in what we'll discuss later as hops or intermedia transactions that are between an origin and a destination transaction or mixers, those all obfuscate source and origin and destination.

On top of that, setting aside those little intermediate steps that are taken, be it hops or mixers, there's new privacy tokens that have started to take the place of Bitcoin in these markets. For example, Monero, which has traded under the symbol XMR, boast a far less transparent blockchain and thus it promises users increased anonymity, right? So, going beyond pseudonymity to true anonymity.

In addition to the currency evolving, we're seeing the black markets evolve as well. Mike hinted at a minute ago, we're moving beyond narcotic sales into murder for hire. In 2023, the DOJ seized a market named Genesis Market, which also cropped up on the dark net and primarily dealt in user credentials, and so the website would acquire user credentials and personal information stolen in malware and/or hacking attacks and sell the same in exchange for Monero, XMR, these privacy tokens, again, which provide a broader anonymity than your typical Bitcoin.

Ethan Ostroff:

All right. So, interesting stuff, Brett. I mean, I guess what's stopping federal agencies from simply seizing the various darknet black market domains that are facilitating this type of illicit activity where cryptocurrency as a payment method is preferable.

Michael Lowe:

Well, Ethan, the problem here is that enforcement is complicated in this space. For one thing, darknet websites are hard to identify. For another, it's really a question of resources because you have so many of these darknet websites that'll just pop up where they facilitate illegal transactions. It's kind of like playing whack-a-mole. The feds can shut down and target and get a court order and seize or shut down one darknet domain, but then another one just pop up.

On top of that, you have to contend with the fact that many of these are located and are operated overseas. Engaging in any kind of meaningful takedown of the site in those circumstances requires a level of international cooperation between US and foreign law enforcement and authorities. Speaking from experience, as someone who's done that, it's a lot of work. It takes a long time. It's not just as easy as snapping your fingers and getting this done. But it does happen.

I'll give you an example there. The Genesis Market takedown that Brett was talking about a little while ago, that operation involved over 400 law enforcement officers across more than a dozen countries. So, short answer is it happens, it takes a lot of effort, and there are a lot of these sites.

Ethan Ostroff:

Sure. So, I guess does that give you a you know, true enforcement here from a criminal perspective is hopeless, because it takes so much cross-border coordination, and a lot of manpower and money, quite frankly, to pull these off, right?

Brett Broczkowski:

Well, like Mike said, enforcement is difficult. I'm not sure we're ready to give up on enforcement yet. In 2022, darknet revenue was down to $1.5 billion from $3.1 dollars in 2021. Homeland Security credits this decrease with ramped-up enforcement efforts of the various federal agencies, as well as the shutdown of major markets like Genesis Market. To be sure, like any criminal enterprise, some darknet participants will remain undeterred by enforcement and will

continue to change strategies and coins to continue their operations and avoid detection and takedown.

Michael Lowe:

While it's true that crypto will no doubt remain the preferred payment method for criminal actors, I think it's equally true that law enforcement has shown that they are dedicated to targeting this space, and they've not only shown no sign of backing down, but they've been, in fact, the opposite. They've been ramping up efforts. So, I think it's just going to be a battle. Criminals will continue to do this, and law enforcement will continue to target it.

Ethan Ostroff:

Sure. I appreciate that. I thought maybe we could turn next to talking a little bit more about crypto-related scams, right? One of the four things you mentioned earlier, Mike. Could you give our listeners just a general sort of overview or a high-level perspective on how these scams often work?

Michael Lowe:

Yes, Ethan. I mean, I've seen many different types and the reality is like any kind of fraud, a crypto-related fraud can vary greatly. Two of the most common that we see now are those involving fraudulent investment websites and those that mimic what would be a traditional tech support scam.

So, for the fraudulent investment website type scam, you find a scammer will reach out to the target, usually through some form of social media, attempt to establish a rapport, and once that occurs, the scammer will recommend it, an investment in cryptocurrency. When you're dealing with people who aren't sophisticated with respect to crypto, it's the allure easy money is just too hard to resist for some people, and particularly those that don't really understand crypto. And you'll find people who all they know of crypto is, “Oh, Bitcoin, it started out at a couple of dollars, and now each Bitcoin's worth $40, $50, $60,000 a Bitcoin.”

You get these fraudsters or these scammers who play upon that and they'll enlist investment in what turns out to be a non-existent crypto investment. They get pretty sophisticated because you'll find websites that designed or are designed to look like legitimate investment companies. In reality, they're not and they're operated by the scammer. Then once the money gets put into the investment account, if you want to call it that, it disappears.

The second form of scam, the scammer will pretend to over-refund someone for tech support-related purchase like virus protection. Scammer will often demand repayment through crypto and instruct the target to retrieve the crypto from a crypto ATM so that they can easily avoid traceability of the digital asset.

Ethan Ostroff:

Yes, I mean, it's always interesting to hear the sad stories of how people actually fall for these types of scams you described. I mean, one I've seen repeatedly this year has been people thinking they were accessing a legitimate crypto exchange only to be duped into it being a knockoff, right? Then in order to try to get their coins or different types of cryptocurrency out of that exchange, they keep being told for some reason or another why they need to deposit more crypto into their account on this fake exchange, right? Only then find themselves just digging themselves deeper and deeper into a hole.

I mean, do we have any sense of how many people actually fall for these scams? These scams are not new to crypto, right? Crypto is just sort of a new iteration of these scams that have been essentially going on for a very, very long time, just changing and evolving over time as there becomes new technology and new opportunities to sort of tweak the process by which they actually get the money from their victim into the bad actor's own wallet, if you will.

Brett Broczkowski:

You're quite right, Ethan. While these scams aren't new, they are indeed prevalent, and the IC3 data bears that out. In 2023, investment scams reported to IC3 resulted in a loss of $3.96 billion to Americans. To put that figure in perspective, the next most prevalent scheme involving personal data breaches led to losses of $494 million. So, these investment scams of what you just spoke, the fake websites made to look like real websites are resulting in catastrophic losses of several billion dollars on an annual basis to Americans.

Ethan Ostroff:

That juxtaposition, Brett, is really interesting. Because I think people are getting more and more used to being aware of and sensitive to the impacts that a data breach can have, right? And are increasingly in the news about various different types of data breaches. But then you look at the numbers and you're like, it's a multiple of eight, right? The dollar figures in losses, it's eight times more for investment scams versus data breaches in this country. That juxtaposition to me is actually quite shocking. Would you recommend that people who are scammed in this way using cryptocurrency seek legal assistance in trying to recover it? I mean, are there things individuals can do outside of the criminal context from a civil context to try to recover that money?

Michael Lowe:

Ethan, I would recommend that people continue to seek legal counsel, but I would make the point that they need to make sure they're using trusted legal counsel, like go to a legitimate trusted law firm. The reason I say that is because there's actually a scam that's going on now where people who've been scammed out of their cryptocurrency have sought out a law firm that allegedly specialized in the recovery of crypto assets. In fact, that law firm was a scam itself. The victims who had already gotten their crypto stolen from one set of scammers reached out to a law firm and were scammed by this fake law firm who promised to help them get their crypto back. And the law firm asked them to basically put in a bunch of upfront fees and back taxes and strung them along and tried to milk them for as much as they could. Literally in, I think, it

was February of 2024, there were reported losses of about 10 million dollars just from that fake law firm scam.

Ethan Ostroff:

That's unbelievable. I mean, it's like by your Google keyword and ad words searches, so when people go into search for a law firm to help with this, they end up getting filtered towards a scam. What can consumers do to protect themselves? Then what about financial institutions? What are things that they can do to protect themselves?

Brett Broczkowski:

Yes. Starting with consumers, we really have three tips. The first is, use your common sense. Don't be allured by the crazy prospect of returns that don't seem realistic. If something seems too good to be true, it probably is. Second, if you're going to invest in cryptocurrency, use a trusted platform. As you said, you're seeing very prevalent scheme involving fake platforms, spoofed to look like real ones. Don't click a link offered to you by a benevolent stranger. Go directly to the website that you know, the trusted exchanges, and use those. And third and finally, look out for those around you. Even if you are a sophisticated investor and capable of spotting and avoiding scams.

As you mentioned are the elderly among us, our elderly friends and family are the ones most susceptible to these crypto-asset scams. Keep an eye out for them. If you hear them talking about the prospect of great return that they were promised, intervene. Make sure they know what they're doing.

Ethan Ostroff:

I would just add to that. I think you made a good point about don't just follow links that someone else provides to you, especially considering the prevalence on social media, individuals making statements about various things and providing links. There've been a whole lot of negative outcomes from using and clicking on those types of links that people have experienced.

It's the same sort of advice that we use all the time and how we try to safeguard our own IT infrastructure, right? Don't click on things from people you don't know. Don't assume that that link provided in an email with what looks at first glance like a legitimate website is so – go on the Internet, type it in yourself, make sure it's legitimate, right?

Mike, any thoughts about what financial institutions might do to protect themselves?

Michael Lowe:

Before I get to that, one point I want to make on these sorts of the consumers being aware is what I'm seeing, a lot of these origins are now in chat rooms. People go into chat rooms and there's a bad actor in the chat room who is trying to direct traffic to either a fictitious website or a crypto asset that is basically set up as a scam itself. The chat rooms are not without risk. You

got to really be aware if you're going to go into them, not to just click on links or believe everything you read in them.

To answer your question about institutions, I mean, with respect to the institution's customers, I think it's really important for institutions nowadays to do all they can to educate their customers and their consumers about the scams that are going on in the crypto space, particularly if the institutions are involved in any way, shape, or form in crypto. Because really, general knowledge about cryptocurrency remains low nationwide and can do a lot just by even providing some basic knowledge to your customer base about cryptocurrency, the risks of the scams that are going on, that can give them the pause that might be necessary to help them avoid becoming victims.

I also think for those institutions that are involved in cryptocurrency, it's really important to do your due diligence to make sure that the crypto assets that you're making available to your customer base customer base are well-known blue-chip assets, if you want to call them that, that any websites or changes that are being used are the trusted well-known exchanges and not the newer coins or the newer exchanges.

Ethan Ostroff:

All right. So, I thought maybe now we could switch gears and talk a little bit about the final category of crypto-related crime that you identified earlier, Mike, money laundering. Start with the basics. How does someone launder money using cryptocurrency?

Michael Lowe:

Unfortunately, for the law enforcement agencies, the process of laundering money via crypto is in many ways even simpler than traditional money laundering. There's been new technology in the crypto space known as the crypto mixer, which is to put it quite bluntly, it's really a tool designed to launder money. Those looking to launder their crypto can deposit it into a mixer where it's basically blended up with other deposits of the same type of a coin through several serial transactions and the funds are broken down into small amounts, recombined several times throughout the process, and then returned to their depositors via entirely new crypto wallets. As a result of that process, the funds become virtually untraceable.

Brett Broczkowski:

As we hinted at earlier, Ethan, these mixers are compounding the enforcement challenges that are already raised by the new privacy token. So, whereas the privacy tokens themselves offer anonymity, now even coins like Bitcoin that have very public and transparent blockchains can be washed and redistributed in untraceable form.

Ethan Ostroff:

This topic is always interesting to me because I think there are people on both sides of the fence as to whether or not the washing and mixing makes crypto qualitatively different than normal fiat paper money in this context, and whether or not it's actually more likely that you can

actually trace the path of digital assets in a way that's better than you could trace good old-fashioned cash in the various types of schemes that are used in good old fashioned cash to launder it.

I still go back. I can't remember when it was, but I think it was in 2023 where there was testimony in front of the Senate and someone who was part of a panel was having a very spirited debate with Senator Elizabeth Warren about that distinction, pseudonymity versus anonymity, and trying to make the point. I think what was well made at the time about why it may be that crypto transactions are actually more easily traced to their ultimate beginning and end, than traditional cash because of the various different tools that can be used, and why that's a lot easier than trying to track suitcases full of dollar bills.

So, I think the use of mixers is at an all-time high. This continues to go up. There continues to be increasing enforcement activity, involving mixers as well, where we see federal regulators going after and trying to shut down different types of mixers. What is the type of enforcement you guys are seeing in this situation?

Michael Lowe:

To address your earlier point, I think you're exactly right. I mean, the difference, though, is that mixers are now what really renders cryptocurrency very easy to launder. Absent mixers, your traditional crypto on a blockchain, you're right. You could basically trace the transactions. But the use of mixers changes all that because now you're literally taking bits and pieces of some crypto assets and combining them with others and getting something entirely new and untraceable.

But DOJ is continuing to address that challenge as well. There were two very high-profile mixer cases brought by the Southern District of New York between August 2023 in April 2024. The first one in August 23 was the Tornado Cash case. It was a case brought against Roman Storm and Roman Semenov. They were charged with operating Tornado Cash, which was at the time a very popular crypto mixer, which Semenov and Storm referred to as a coin anonymizer. That Tornado Cash operated as follows. Users were basically instructed to deposit their tokens in predefined increments, which made them easier to break down and recombine. They were basically given a secret note that would permit them to later withdraw the laundered crypto. And Tornado Cash instructed the users even to wait several days before withdrawing the crypto to further disguise any link between their deposit and the withdrawal.

At the time of the deposit, users were even showing statistics on how many other deposits were made into a given pool of cryptocurrency, which would let them know the difficulty that would be associated with tracing their deposits. Essentially, the idea was users send some coins in and they take different coins out.

Now, one thing that's significant in all this, and which I think is part of the problem with regulating cryptocurrency exchanges is that Tornado Cash had no know your customer, no AML programs, they weren't registered with FinCEN, they didn't file SARs, and they didn't comply with the Bank Secrecy Act. So basically, what you had was a business that was essentially really set up to launder money. The government alleged in the indictment was that Semenov and Storm intentionally declined to adopt any of those programs and that they knew that

Tornado Cash was being laundered, was being used, and the government also alleged that they knew that Tornado Cash was being used to launder money. This is where cryptocurrency laundering has headed. I think Brett's going to talk about the other case.

Ethan Ostroff:

So, wait, before we move on, just real quick, correct me if I'm wrong, but I don't believe that criminal cases reached a conclusion, right?

Michael Lowe:

Correct.

Ethan Ostroff:

So, what we were just describing, that's the allegations from the indictment about how the process worked according to the government. Yes?

Michael Lowe:

Yes. It's not all that. I think that's how it was listed on when you went on Tornado Cash. These were the instructions you were given. But yes, this is an ongoing criminal case, so these are allegations that the government has made.

Ethan Ostroff:

There's a lot of debate in the digital asset world about whether or not this is really something individuals are doing or whether or not this is computer code that was created and is running and whether or not these individuals can be really charged with these crimes as if they're committing these acts. There's a lot of debate about not just Tornado Cash, but the way other types

of mixers work as well, and whether or not obligations of anyone, if it's simply computer code, to comply with these various laws.

Michael Lowe:

I would agree with that. What it always is going to come down to Ethan is a question of intent here. One of the key facts, I think that the government is relying upon, they alleged in their indictment that there was a September 2020 hack of a crypto exchange where it was widely reported that millions of dollars in stolen assets went into Tornado Cash, and the exchange actually emailed – these are allegations, the exchange email Storm and Semenov and asked them to help to block the proceeds, but they refused.

There was another hack in 2021 where another two hundred million dollars from another exchange was allegedly deposited into Tornado Cash. So, the government's allegations with respect to Semenov and Storm are that they were well aware that illegal proceeds were going

into their app to their Tornado Cash mixer and the new was being used to launder those proceeds and they refuse to do anything about it.

So, when you start adding in the level of intent and knowledge, I think that's where you find these mixture developers running into problems with federal authorities.

Ethan Ostroff:

Sure. So, I guess any other, Brett, notable enforcement efforts in this particular context that you might want to bring to the attention of our listeners?

Brett Broczkowski:

Yes. Actually, in April of this year, the DOJ charged Keonne Rodriguez and William Hill with operating another popular crypto mixer called Samourai Wallet. And the case looks very similar to Tornado Cash. Samourai, they blended fixed-amount transactions of cryptocurrency, breaking down and recombining the amounts and then redistributing them into new wallets for these individuals. They also offered a service. We mentioned this earlier. The service was called Ricochet, and what it did is it created unnecessary hops or transactions between an exchange of cryptocurrency. Even if you're trying to get crypto from A to B, they would add in several different intermediate transactions to try to further disguise the origin.

All told, about $2 billion worth of Bitcoin passed their samurai wallet, and $100 million are alleged to have been involving criminal proceeds, 1,500 Bitcoin alone were processed from transactions involving darknet markets like Silk Road. So, like the founders of Tornado Cash, both Rodriguez and Hill were charged with conspiracy to commit money laundering and conspiracy to operate an unlicensed money-transmitting business.

Kind of the color what Mike was just talking about, the indictment goes on to kind of spell out the clear or what the government believes are the clearer hallmarks of intent, right? So, they had no anti-money laundering compliance programs, no know-your-customer or BSA compliance. They weren't registered with FinCEN. Then, to take it a step further in this Samourai Wallet case, one of the owners, Rodriguez, operated a Twitter account that had tweeted encouraging users to launder criminal proceeds through the app.

At one point, Rodriguez and Hill had even invited Russian oligarchs to use the app. So, these are kind of the pieces of intent that the federal authorities are looking at to say, “You knew this platform was being used to launder criminal proceeds. It was not simply a privacy service as it was billed.”

Ethan Ostroff:

I've always thought one of the most interesting things about the Samourai Wallet is the perceived divergence between FinCEN guidelines and what the DOJ has alleged and stated in its indictment, because it seems like they're kind of irreconcilable, right?

Michael Lowe:

Yes, I'd agree with that. Basically, DOJ is essentially saying, yes, FinCEN's guidance is just FinCEN's guidance, and that does not provide a defense to the charges. Really, I think the clearest distinction as Brett and I are both talking about is, it comes down to a question of intent, and if the government can prove that you knew that your crypto mixer is being used to launder proceeds, and they're going to work hard to get that evidence of intent, then I think you're really at risk of being prosecuted for money laundering.

Ethan Ostroff:

Sure. That makes sense. I guess, in light of that discussion, I guess any sort of final thoughts about risks that financial institutions should be aware of in this context of the use of mixers and money laundering?

Michael Lowe:

Ethan, one of the largest risks, I think, for financial institutions is ensuring compliance with anti-money laundering and know your customer laws. The use of crypto mixers can place an increased compliance burden on your traditional financial institution. Think about the difficulty of rooting out the proceeds of a theft, and that sharply increases by the threat of washed and untraceable crypto assets.

Brett Broczkowski:

Yes. Where crypto assets are stolen, sent through a mixer, sold into fiat currency, and then deposited into a traditional financial institution, that institution has to rely on information from various decentralized external sources to try and identify which funds were stolen, let alone to who they rightfully belong. So, kind of like the enforcement problem that the government is facing where it has to piece together information and task forces from several different nations and across hundreds of agents, these financial institutions are having to piece together information from various decentralized sources to try to identify the source and rightful owner of these funds.

Ethan Ostroff:

The final thing I want to talk to you guys a little bit about is the FinCEN guidance on this topic. I will say I do want to gently push back on the notion of these assets being untraceable. In my mind, I keep going back to the idea that it may be a different process to trace them than what we and, quite frankly, the government and prosecutors are used to. But I've got to think that I have a much better chance of tracing crypto assets through various wallets, exchanges, and even mixers, as opposed to suitcases full of cash being handed off from person to person or being put into the register, the till, if you will, at business number one and then move to business number two.

I mean, to me, I think there's reason to push back on this narrative about lack of traceability. That to me, I still come back to the idea that the traceability is different, but does it mean that it's

less or worse than what we have traditionally been dealing with in the money laundering world when we talk about the movement of cash and how difficult it can be to actually follow the movement of paper bills.

But let me just move on now, and I appreciate you guys talking through these various topics. They are very timely and interesting. The FinCEN guidance on this topic, so maybe just begin with

reporting obligations, and the type of reporting financial institutions must do if they notice something suspicious involving crypto.

Brett Broczkowski:

Yes, so an institution who notices something suspicious involving crypto must file an SAR or suspicious activity report. That report must typically be filed in 30 days of the suspicious activity of the institution noticing that activity. And the guidance requires reporting of any transaction of at least $5,000 that the institution knows or has reason to suspect involves funds derived from a legal activity, is designed to evade the requirements of the Bank Secrecy Act, has no business or apparent lawful purpose, or involves the use of the financial institution to facilitate criminal activity.

Ethan Ostroff:

Okay. Has FinCEN provided any tips for what institutions should look out for to try to identify the situations where they have an obligation to file an SAR?

Michael Lowe:

Ethan, yes. In fact, they have. FinCEN actually published a series of red flags that institutions should be on the lookout for. A few of those are customers with no crypto history, suddenly exchanging large amounts, the use of traditional loan vehicles to purchase crypto, crypto transactions that are linked to darknet markets, and customers who mention an interest in a lucrative crypto opportunity. Those are just some of the things FinCEN says are red flags that institutions should be aware of.

Ethan Ostroff:

That's great. Thank you so much. Mike, I really appreciate you all joining me today for this episode of *The Crypto Exchange*. I want to thank our audience for listening to today's episode as well. 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 platform you use, and look forward to our next episode.

Michael Lowe:

Thanks, Ethan.

Brett Broczkowski:

Thanks, Ethan.