diffuse*tap*
Virtual Event Series

Chasing Crypto Scammers

Guest Speaker:

David Croft
Partner at Meyers, Roman, Friedberg & Lewis

Hosts:

Kenny Estes
CEO & Founder
Diffuse

Ayla Kremb
COO & Co-Founder
Diffuse

DiffuseTap: Chasing Crypto Scammers

Last time on DiffuseTap, **David Croft, Partner of Meyers, Roman, Friedberg & Lewis,** talked to us about the framework and lifecycle of a typical crypto scam, why perpetrators of crypto scams are generally hard to track down, and what options do victims have in recovering their stolen assets.

Want to make friends from the Diffuse Fund Ecosystem? Email contact@diffusefunds.com.

DiffuseTap

This networking session is part of our weekly virtual events series. Networking (you'll bump into at least a dozen high caliber fund managers) meets purposeful (you'll tap into brand-new sources of ideas)... straight from your armchair like a boss.

Meet the Speaker

DAVID CROFT has more than a decade of legal experience in blockchain applications. He is currently the Chair of Meyers, Roman, Friedberg & Lewis' Blockchain and Cryptocurrency Practice Group and has also worked as General Counsel and COO. David is an expert in a wide range of spaces, from cryptocurrency, cybersecurity, data privacy, medical marijuana, software, and manufacturing. LinkedIn: @davidvcroft

About Diffuse®

We are an alternative fund platform offering differentiated investment products. From digital assets to VC funds and beyond, we identify green field investment opportunities we feel will have market beating returns and turn them into professionally managed funds. For more information, visit www.diffusefunds.com.

KENNY ESTES: Mr. Croft, would you mind telling the good folks a little about your background and what you're up to now?

DAVID CROFT: Sure. Thanks, Kenny. Thanks, Ayla. I'm happy to be here talking to everyone today about crypto scams. I am an attorney based out of Cleveland, Ohio. There are not a lot of attorneys working in crypto and blockchain up here, so I'm a little bit on an island by myself. I got started with digital currency with in-game brokering clients around 2005 or 2006. And then, I got involved in crypto and blockchain around 2011 or 2012, personally and professionally.

It doesn't seem like a long time when you look at it from a numbers standpoint, but it feels like a very long time being in the industry, with all the different machinations that have occurred everywhere from mining, to the ICOs, to security concerns. And now, I think what fills most of my time in the crypto space is getting calls from folks that have been scammed, so to speak.

That's primarily what we spend a lot of our time with nowadays. We still represent clients that are starting businesses in this space, or that are currently operating businesses in this space. But primarily, it is with cryptocurrency scams. I'm happy to talk about what is and what is not a scam, because we've seen many different situations.

AYLA KREMB: We can kick off from there. What constitutes a scam and what does not?

DAVID: Okay. Let me start by saying that when I get a call from someone, it's usually in two big buckets. The first bucket, which I would say is not a scam, is when someone has funds invested on a legitimate exchange, and they cannot get them off. They can't contact anyone. The most recent case I had was a client who is living in the US, but does not have a social security number. This particular client has a significant amount sitting on Coinbase. When he tries to pull it out and they go through the KYC, and AML (that's Know Your Customer and Anti-Money Laundering requirements), he has an ITN instead of a social security number, which doesn't fit in the box.

As most of you that have probably dealt with Coinbase or Kraken or any of the other exchanges know, in those cases you're dealing with a chatbot. And if you're not going to fit perfectly in that box, you're not going to get any attention unless you hire a law firm to start writing letters to get a human being's attention to help you do whatever it is you're looking to do. That's one bucket. But those are really not what I would call a scam.

Also in that bucket are situations where someone's account may have been hacked because of a mistake or an omission by those exchanges. The vast majority of the folks that I talked to in the other bucket are folks that are calling me because they put their life savings into something. And now, that something has disappeared.

Another case is that they've got an individual who they really trust that got them to invest a small amount , and then a larger and larger amount, and that individual is now asking or has asked them to

put a significant amount in to pull out all of the crypto that they have currently sitting, wherever it is. I get those calls from people who are either worried or who have already been scammed, and they're looking for someone to help them.

KENNY: That makes a lot of sense. I hear a lot about rug pulls. Correct me if I'm wrong, but my understanding is that in its simplest form, a rug pull is when you use a smart contract, they put a backdoor in there and they use it to exit with your funds. How does that work from a legal perspective? Because obviously, a smart contract is not a legally-enforceable contract. You don't sign terms of services. So, is that considered a scam? Is that illegal? What does that landscape look like?

DAVID: It's a scam, certainly. I don't know if there is a statute that defines a scam but really, what you're looking at is theft or fraud. Those are all legal concepts on the criminal side. You've got criminal and civil dichotomies here. If you're able to identify the individual or entity, and you're able to bring a lawsuit against them in civil court, that would be a civil matter.

You're not seeing a lot of scams there because most of the time, individuals can't identify who stole their money. They're usually working with someone that is working under a false name, or a false company that doesn't really exist. And by the time they come to me, that entity or individual has disappeared, and there's no way to track them down other than involving law enforcement.

AYLA: What about investigators? Do you think too many people get their own private investigators to start looking into cases, identify individuals, and make sure that at least they have the person that stole their money on hand?

DAVID: Some folks do, most folks don't. They're immediately reaching out to an attorney because their thought process is that the attorney can help them somehow. And very often, it's difficult for us to help individuals that have been scammed by someone that is overseas. That is unidentifiable and untrackable. Unfortunately, some of the things that draw a lot of us to the crypto space make it very, very difficult, or almost impossible to track these criminals.

We've got a decentralized organization or decentralized system. There's no oversight from a bank or a government. It's very attractive, but it also can be detrimental to folks that have been scammed. Transactions are irreversible. Once it goes from one wallet to the other, there is no mechanism to pull them back in most situations. And then, of course, one of the favorites of crypto criminals is that it's pseudo anonymous. It's not 100% anonymous, but it's very, very difficult to find out who this person or entity is and track them.

KENNY: Okay, that all makes sense. It sounds a bit doom and gloom in this space. One more question about that and then we'll jump to the questions in the chat. If somebody does experience a rug pull, what do you recommend to them as the course of action given that you might not necessarily be able to help? What's your advice for somebody going through that?

DAVID: First and foremost is involving law enforcement. I will say that it's very often that law enforcement is not able to affect a result. You've just got a huge volume of reports for many different things in it. Individuals are likely going to file a claim with the FBI and the federal government under iC3.gov. Once those claims are filed, it goes into a system where an investigation is started. Or, if there are enough incidents involving a particular threat actor, it might get special attention, or perhaps if there is a significant amount involved.

But very often, you've got not enough agents with not enough resources to track down whoever the threat actor was. I would say more than half of the clients have already contacted the FBI, or contacted their local law enforcement agency that may have a cybersecurity division. And after having filed these reports with no solution, they're left with nowhere to go.

My suggestion to those individuals is usually twofold. One, contact your accountant. The IRS defines cryptocurrency as property. I know that we've got numerous federal agencies defining cryptocurrency as different things. Securities, commodities, the list goes on. But the IRS looks at it as property, at least most recently. One of the things that an individual may be able to do is take advantage of this as a loss of property from a tax standpoint. And so, I encourage them to speak to their individual accountant and tell them about what happened. Try to take that position and see if it's helpful to them.

The other thing is not always successful. In fact, usually there are fights involved in this. It's to report a loss of property to your homeowners insurance. Or, if you've got another type of insurance policy that may cover this type of loss, report it to them. Now, insurance companies have become wise to this and they are taking the position that this is the same thing as investing in Verizon or Apple and losing your money in that investment, and it's not going to be covered by your homeowners policy.

So, what is left there? Well, you can hire a law firm to take a look at that policy to see if there's any wiggle room there. If there's a potential fight, maybe you can settle something with the insurance company to at least get some of your money back. It's largely doom and gloom, but there are some possibilities out there for partial recovery. I would recommend those three steps. Go to law enforcement, then talk to your accountant, then see if there's anything that can be done from an Insurance standpoint.

AYLA: What kinds of scams do you see most of these days? What is the top tier?

DAVID: I'm saying this having gone through the ICO craze, which I think the SEC has put a damper on because of all the rug pulls and ICO scams. Nowadays, it's mostly threat actors overseas and using what a lot of cybersecurity criminals do. They use social media. They use psychology and social media to gain the

trust of individuals. And once they've gotten the trust of those individuals, they encourage them to invest in a foolproof, get rich quick scheme.

And so, these individuals will invest a small amount of money. Small, I guess, is relative depending on who you're talking to. It can range from a thousand to a couple thousand dollars. Those individuals invest that money and they see a 100, 200, 300% return on their investment almost within a week. The threat actor immediately allows them to withdraw those funds, and then goes back and says “I've got a much better investment for you to do, but it's larger, and the rewards are much larger.”

It goes on and on that way. And perhaps the threat actor disappears after the first or second round, but sometimes you see it in the third or fourth rounds. And oftentimes, these individuals get so far in over their heads, they're taking out lines of credit on their home equity. They're taking out loans from their 401K. Their life savings are being dumped into this. They're borrowing from friends and family.

And after that, you'll see one of two situations. The individual will disappear, or they will continue to try to pull money from the victim by saying “we owe $40,000 in taxes” or some other arbitrary number, and “you have to pay that in order for us to release these funds to you.” That would probably be the last bite at the apple for the threat actor. I would say that the IRS is never going to collect through a third party like that. Individuals that owe taxes on these types of things will be paid directly to the IRS.

That's usually what we see most of nowadays. And unfortunately, you're typically dealing with overseas threat actors that are very hard to track, and they're only going to be high targets or very high on the radar of law enforcement if they're doing this a lot. There are some that tie to criminal organizations or terrorist organizations, or some government that is not friendly with us.

KENNY: Gotcha. That makes sense. I've started watching the Bernie Madoff Ponzi scheme scandal on Netflix and it sounds very similar to that, but with new technology tools. A question from the chat here. This might be a little too specific, so feel free to differ. FTX and SBF are all in the news right now, including the FTT tokens which seem to have not been well managed. Is that fraud in your opinion? Does that rise to the level of fraud, or is that just straight up mismanagement and poor business decisions?

DAVID: Oh, that's that's difficult to say at this point. Anything that I would say would probably just be a personal opinion based on what I've read, just like everyone else here. I think the demeanor of SBF and everything that has happened to date could rise to the level of fraud.

Again, we're dealing with concepts or legal theories that may have different thresholds depending on the laws that are applied, whether it's federal or state. My opinion here is I think we will likely see some fraud here. I don't think it's going to stop at mismanagement. It's just too much of the loss in some of the things that just look pretty shady from an outsider's point of view, from reading articles. I didn't really answer the question, sorry.

AYLA: Well, I think we're all guessing in that whole situation. In terms of recovery for victims, in the landscape of actual recovery from the scam and also insurance recovery, how often does recovery actually happen?

DAVID: If you're looking at the whole landscape, usually the recovery for victims from the scam is zero. It's almost never solved unless you lost six figures. Plus, it's almost never ending. I would say the vast majority of folks out there are losing in tens of thousands. It's not sophisticated investors. They're not taking their time to look into what it is they're investing in, and they're immediately giving their funds out so that the savings that they have available at their disposal is going to be tens of thousands. From a scam standpoint and from a law enforcement recovery standpoint, it's almost zero.

From an insurance recovery standpoint, I would say you're looking at 20 to 25%, or probably larger 5 to 10 years ago. That's because insurance companies were just starting to get involved here and the SEC had not taken as strong a position as they have recently. And so, the insurance companies are all pointing to Gensler, and the SEC is saying that crypto is a security. Therefore, it's like losing money on the stock market. They're not going to cover you.

KENNY: Gotcha. One last quick question for you. You mentioned law enforcement, and the FBI comes up a lot. Do they have dedicated resources that are pursuing these types of cases or building out a new program? What's the state of play there?

DAVID: I've spoken with agents that are focused on the crypto area. To that end, I would say that there are some dedicated assets that are focused on this, but I'm not aware of a specific crypto department. I know that there is a larger cybersecurity group out of Seattle. I'm actually going to be speaking to them later today as I also do cybersecurity breaches. I cover all kinds of breaches and any kind of scam on the internet, or anything that would fall under that umbrella. But I'm not aware of a cryptocurrency-specific group or committee or department within the FBI.

Thank you for downloading this DiffuseTap event transcript.

Sign up for upcoming sessions and check out past features and event transcripts.

Dennis Chookaszian

Corporate Director, CME Group

DiffuseTap: Institutional Grade Governance

Sharing his decades-long expertise on corporate governance, Dennis talked about how to avoid a co-partnership going sour, the problem with overly idealistic CEOs, and the importance of keeping your board in check. Read on

Susan Brazer

CEO & Founder, LionShare Media

DiffuseTap: Media Metaverse 2022

Susan described the 2020 digital media landscape; the evolution of media distribution; how converging, emerging technology points to the metaverse; and the prospect of having an open, decentralized, and free Web 3.0 marketplace. Read on

Raj Mukherjee J.D.

VP/Global Head of Tax, Binance.US

DiffuseTap: Crypto Taxes Decoded with Binance.US

Raj explained the complexities of the US crypto tax landscape, how he built a dynamic tax information system for Coinbase and Binance from scratch, and how investors can profit from crypto without getting caught in a taxation mess. Read on

JOIN US