FTC Decrypting Cryptocurrency Scams Workshop
June 25, 2018
Segment 3
Transcript

DUANE POZZA: I'm happy to introduce our third panel, which is called Effective Approaches to Cryptocurrency Scams. We'll be talking more about some enforcement strategies, consumer education, and anything more that needs to be done in combating cryptocurrency scams. My name is Duane Pozza. I am an assistant director in the division of Financial Practices. Just one reminder, if there are-- if we have time at the end for audience questions, we will do those. So if you have questions in the middle of this panel, you can write them down on a note card and just hold them up. And we have someone who will be periodically scanning to see if anyone is holding up a notecard, grab it, and then we'll see if we have time for questions at the end.

So I'd like to just give a brief background of our distinguished panelists. Michael Frisch is at the CFTC. He's a senior trial attorney in the Division of Enforcement. He's based here in Chicago and works on cryptocurrency-related investigations and enforcement actions, including those involving market manipulation, fraud, and trade practice violations.

David Hirsch is at the SEC, where he is the cyber liaison and a senior counsel in the Fort Worth office. He's an enforcement attorney and also a member of the SEC's DLT working group, and the dark web working group. Sarah Jane Hughes is the University Scholar and fellow in commercial law at Indiana University's Maurer School of Law. She's also a veteran of the Federal Trade Commission. Since 2014, Sarah Jane has served as the reporter for the uniformed law commission's work in this field.

Colleen Sullivan is the chief executive officer of CMT Digital Holdings. In her role as CEO, she oversees CMT Digital's trading investments and regulatory initiatives in the crypto assets and blockchain technology space. So I think a natural place to start this panel is to talk about enforcement actions, although that won't be the only thing we talk about. And I thought since we have some representatives from agencies that have done work in this area, we could start there. So I'll start with Mike, actually.

And this is a question for Mike and Dave. You can decide who gets to go first. Both of your agencies have obviously been active in the area of cryptocurrency fraud. And I'm wondering if you could just talk about what your agencies have said about their role in combating crypto frauds in this area and some of the work that's been done?

MICHAEL FRISCH: OK, I guess I'll start with the standard disclaimer. So I'm Mike Frisch. I'm speaking here not as a representative of the CFTC, so any opinions I give are my own. So we have to say that for all of our presentations. So on February 6, 2018, Giancarlo, who is the chairman of the CFTC, testified before the Senate Banking Committee. And there are some prepared remarks you can download off the internet if you want to see what he said there.

I think he gave a nice overview of how we view our role. So you know, unlike a security or a futures contract, there's no one regulator that's responsible for cryptocurrencies. So the CFTC, the position we've taken, is that Bitcoin is a commodity. Other cryptocurrencies are or can be a commodity. And our role is to investigate and, if appropriate, take enforcement action against firms in the space that are offering derivatives on cryptocurrency, futures contracts and options, and also companies that are involved in fraud and other kinds of market manipulation, both in connection with derivatives and also in the spot market.

So I guess what that means is we have a pretty-- we view that we have a pretty important role to go after this kind of bad conduct. But unlike our role with respect to futures exchanges, like the see me down the street, we don't have regulatory authority. And I think that's really important for people to remember when they're buying cryptocurrency on a Coin base or some other exchange. You know, we don't set rules for how money is, customer money is held.

We don't set rules for how trades are processed. We don't set rules for a host of other things that do exist in the regulated markets. So we have anti-fraud authority, that's pretty broad. But when it comes to the spot markets, our authority is basically just fraud and manipulation.

DAVID HIRSCH: And to echo what Michael had to say before I begin, the Securities Exchange Commission disclaims responsibility for any private publication or statement of any SEC employee, such as myself. The speech expresses my own views and does not necessarily reflect those of the commission, the commissioners, or agency staff.

MICHAEL FRISCH: His was better than mine. I will adopt that one as well.

DAVID HIRSCH: So the SEC has been fairly outspoken on the issue of cryptocurrencies, and also more accurately or more specifically, digital tokens. And the language we use, I think, is important. So cryptocurrency is to the extent it's just a one for one medium of exchange, something like Bitcoin. And we have not, I think, publicly taken an opinion one way or the other. But the extent is just an exchange of value. That is potentially a currency and therefore more likely, potentially, in the kind of wheel house of the CFTC.

And we, as an agency at the Securities and Exchange Commission, our first inquiry is jurisdictional. You know, is this a security or an investment contract such that we are the appropriate regulator to be involved and the appropriate person to be opining or to be assigning regulatory obligations to the players? Our chairman has been very outspoken on the topic of ICOs and ICO enforcement. And he's basically said while it is theoretically possible for an ICO to not be a security offering, as of a few months ago or as of, I guess, December, I think when he made the statement, he had never seen one like that.

So a lot of the ICOs bear the hallmarks of investment contracts. The analysis we run through is called Howie test. It's based off a 1940s Supreme Court case that basically said, if you are investing money with the expectation of profits, based on efforts of a third party, and that's not like an investment contract, it's a lot like a security, the SEC regulates those. And that creates obligations for the people who are promoting them. The promoters have to register with us. And that is very helpful for investors.

We are a disclosure-focused agency. And we can help protect investors by requiring people offering investments to disclose who they are, where they're based, what their prior experiences are like, setting limits and rules as the types of projections and statements they can make going forward. And so we, as an agency, have taken enforcement actions against people who have violated our rules, primarily for fraud, but also just for a registration violation.

There's a case called Munchy that came out in, I believe, November of last year, where it was basically an entity that was promoting its own internal digital token for the purpose of creating this new network of restaurants and consumers of restaurants, and reviewers. And they thought it'd be great to have this token that would work within their app that was available in the app store. And they had an ICO where they were going to sell these tokens out to the public. And we got involved and brought a settled cease and desist action against them were they acknowledged-- well, they neither admitted nor denied-- but we alleged that they had violated securities laws because their token was essentially a security and they hadn't registered with us.

So we are looking both to try and enforce registration obligations on the promoters, and also seeking to bring enforcement actions against scams and fraud.

DUANE POZZA: And what are some examples, just sort of briefly at a high level, of the kinds of frauds that the agencies have gone after in this space?

DAVID HIRSCH: So I was an investigator on a team that brought a action against a company that was called Arise Bank, which was an ICO that came out in December, was open through January, and we announced our action against them in early February. We saw it and awarded a temporary restraining order against them. They were a company that claimed to have raised upwards of $700 million. They said that their promoters were important members of the community. They said they had relationships with companies that would allow them to issue Visa cards, Visa branded cards, that would allow you to spend any of 700 different cryptocurrencies anywhere that would accept a Visa card.

And we were able to bring forth evidence suggesting those things were false. And they've since made filings in court suggesting they only raised about $3 million, so significantly shy of the $700 million they'd been telling people. So I think we are focused on bringing actions against companies that misrepresent either who they are, what they're doing, how far along in the process they are, or what the likelihood of returns are.

MICHAEL FRISCH: Sure, I'll speak to that. I want to echo a few things that David said. So the CFTC has been working really closely with the SEC on these matters. And I think that's important because we do have very different spheres of responsibility, whether a coin is being used like gold, or like a trading vehicle, or as an investment vehicle, as David explained. And you know, with the CFTC, it's the same thing. The first issue is always, do we have jurisdiction over this conduct.

So when the Ponzi schemes are caught and show up in court, I found that they-- as we've seen-- they often want to spend a lot more time talking about our lack of jurisdiction over their conduct, rather than what they were doing wasn't actually fraud. So we've had a couple of waves of cases.

You know, in 2015, the first case came down. It's called Coin Flip, where the company was basically offering futures contracts and options-- I think it was options on Bitcoin. The commodities exchange act prohibits anybody offering futures or options without being registered with the CFTC.

So it was plainly illegal. The firm shut down and they weren't fined. I think, basically frankly, because it was the first case. I brought a case in 2016 against a trading platform called Bitfinex, where they were offering leverage margined trading to US customers. You can't do that under the Commodities Exchange Act unless you are registered with the CFTC, which they weren't. So that was the case that I worked on.

They stopped doing that and then pay the relatively small fine, $75,000. And we noted their cooperation in the settlement order. So those sorts of, I think, those cases fit into the whole derivatives on cryptocurrencies being offered in a legal way. There was no allegations of fraud in connection with those two cases. The next wave really ramped up when the price of Bitcoin took off in 2017. And we brought a number of cases, I think, eight or nine, don't quote me on the count, of firms making fraudulent promises.

You know, there's a case called Gelfman, where they were offering, you know, promising like pretty much the standard Ponzi pattern, promising huge returns, sending false trading statements when there was actually no trading going on to customers, and then claiming that there was a-- Mr. Gelfman created a fake, allegedly, hack where everyone's money mysteriously disappeared. But in reality, there was no hack and he had misappropriated the funds. So there's been a number of recent sort of Ponzi scheme-esque cases that we've seen a lot of those.

And we've been going after those under section 60 and rule 180.1 of the Commodity Exchange Act, which gives us jurisdiction to go after fraud and manipulation even when there's no derivative involved, which I can discuss if you want, but it might be a little too wonky for this group.

DUANE POZZA: We might come back to that.

MICHAEL FRISCH: OK.

DUANE POZZA: So clearly there's, for the agencies, different jurisdictional hooks. And there's different agencies involved in this area. And we also heard in the last panel from Joe about the states being very involved in the space as well. We heard in opening remarks that the FTC has brought cases in this area and under section five, [INAUDIBLE] practices law. Sort of a two part question that I'll direct to Colleen and Sarah Jane first, which is, are there gaps between what the agencies are doing? And alternatively, are there no gaps and there needs to be? Or what is the ideal level of coordination among the different folks and regulators who are concerned about this space?

COLLEEN SULLIVAN: Sure. So addressing the gap first-- and I feel like I should say that I am here with these regulators and former regulator. I'm speaking on my own behalf and not necessarily my partners at CMT Digital. But I will say when we started trading in the space, a significant gap in regulation, which Michael mentioned, is that there's the spot markets don't have a federal regulator sitting on top of them outside of FinCEN. And FinCEN would only cover certain aspects of what these crypto exchanges are doing.

So our view on trading in the market place was, we've traded for 21 years in regulated markets on regulated exchanges and regulated products. So we did a gap analysis, you know, what are we used to doing in these traditional markets versus what is it like on spot markets, the crypto spot markets? And we developed our own internal best practices and standards and decided that those were the ones that we would hold ourselves to.

So to provide a specific example, you know, unlike our traditional markets, you don't have a prime broker sitting in between the trading firm and the crypto exchanges. So your counterparty risk is to each and every crypto spot exchange that you trade on. So we developed, at this point, it's over 60 points in our questionnaire to evaluate counterparty risk, starting with basic things like, do you know who the management team is? Do you know where they're located? Have you spoken with them?

Really basic stuff. But then it gets into hacks. What's the cold wallet versus hot wallet storage policies and procedures? What's the banking relationship? Is this spot exchange regulated in a foreign jurisdiction? Have they had any enforcement actions? All of that. And then the exchange will either get a yes or no as to whether or not we're on board. And then we further go into how much crypto and fiat are we comfortable leaving on those exchanges? And that's a dynamic risk assessment that goes on daily.

So that's how we've addressed that gap. What we're excited about, and Commissioner Quinn Pence has spoken about, is that Gemini is trying to put together the virtual commodity association, which is a self-regulatory organization for crypto exchanges that trade crypto assets that are deemed commodities. Generally, though, I think that's what we're seeing the industry start to do is self regulate where there's gaps. You know, I think Amy mentioned the Token Alliance with the Chamber of Commerce. There again, you see this push for standards and best practices. And that's really what the industry needs to do to protect itself.

SARAH JANE HUGHES: Last disclaimer of the day. I do not speak for the trustees of Indiana University or for the other faculty members of the Mauer School of Law at Indiana University in Bloomington, or for the Uniform Law commission. It's just me. And it will just have to do. And before I say anything else, I would like to have a show of hands, if that's OK, Duane? How many of you are lawyers?

OK, how many of you are investment advisors or people in financial services companies that are actively involved in this area? Actually, I was they would be a few more of you in this room. And I was hoping that there would be a few more of you in this room, because I think that's part of where some solutions, like industry self-regulation are going to have to come from, a multi-point approach to whether you as an enterprise-- your own enterprise-- whether you're going to partner with somebody, invest in somebody, acquire somebody, merge with somebody, that's a way in which you can help prevent fraud that affects enterprises and consumers at the same time, in my view.

And so how many of you thought you knew something about ICOs before you came into this room? Notice I used the word thought. OK. And then the next thing I want to know is how many of you learned something that you never imagined you would learn already today? That should be everybody, I suspect. But we haven't finished doing-- me too. We haven't finished doing our job yet, when we haven't done those kinds of things. The FTC-- and I worked there from 1974 to 1988-- does two things in addition to law enforcement. But it does two things really well. It does really great business education and really outstanding consumer education.

And I think in all of these arenas, more of both are needed. So I'd like to see more work, like your work. And yours is proprietary. But there are some touch points that could be public touch points for business education in this area so that businesses won't make some of these same mistakes because I fear that they are. And then I would like to just quickly talk about the fact that I think this is a multi-profession role, in terms of dealing with scam artists.

And the FTC has been involved in combating consumer fraud for at least 50 years. And when I joined them in 1974, there were several active cases. Some of those cases were about selling land that was 50 or more miles from the closest energy source, water supply, or it was under water, as investments. And it's-- Howie was an orange grove, if you didn't know that, in Florida. So the FTC and the SEC have been involved with cases like this for a long time.

The next kind of scam that came up involved business opportunities. And the one that stuck with me, which I think came from the Chicago regional office at that time, was someone who was offering franchises to grow mushrooms in your closet. Not like orange groves, but it's close. And then there were the free travel offers. And this was so long ago. And the first of those cases I brought here in the Northern District of Illinois with partners from the Chicago regional office and the US attorney's office here in Chicago. Were free travel offers but it was so long ago that they sent postcards to the intended victims.

And the victim called them because telephone war rooms hadn't really grown up because telephone calls were really expensive in the 1980s. Whereas if you got them to call you, it was free, unlike cell phones for a while. And then there were other things that went beyond that. But the telemarketing from Canada, telemarketing from other places, the stories are remarkably similar across a 50 year history. But there's one more-- there are two more big similarities.

One is, some of these people don't stay in business in the same name very long and almost all of these waves or iterations of scams involve some of the same people. So chasing these people across state borders, across international borders, figuring out how they were getting paid, talking to the credit card companies in the '80s because that's how they were getting paid in the '80s, looking at ACH transfers and other means by which people were receiving money that they took and ran with. And almost everybody has seen that movie The Rainmaker where the insurance company that wouldn't pay for the cancer treatments, eventually the guy ran to Switzerland after the judgment came out. That's what would happen.

So we started doing it-- I did-- I tell my students, including some who were just in the room, that one of my favorite things to do was first we froze their assets with an ex parte government order issued by a judge at crack of dawn. Then we'd find the US Marshal. Then we'd go get their bank account. And then you would serve them the papers saying that they'd just been sued so they couldn't touch the money at that point, so it was the only effective way to do some form of consumer restitution. That piece of this is new and it will be much harder to do that in this space, because it will be much more difficult to figure out where the money is going.

So that piece of the catch me if you can is the one that is the biggest challenge for those who are going to engage in enforcement in this area, in my personal opinion. But that means that we can't let it go that far. We have to try to head it off in a different direction with education, with more robust standards about who's going to invest, or buy, or partner with, and things of that kind, unless they're just pure frauds. I don't think we're going to fix the pure fraud problem. This is just the latest iteration of the pure fraud problem.

That went on longer than I meant, Duane.

DUANE POZZA: Well, just picking up on that--

DAVID HIRSCH: Yeah, if all right, I would just like to echo what you have said. The goal of fixing the pure fraud problem is a very difficult one. I admit it's daunting. But I think the FTC is doing a great thing by bringing people together here and virtually to become more educated about the potential for the pure fraud problem. At the SEC we have a robust program on investor.gov that offers lots of guidelines and things to look at when you're thinking about investing, if you're thinking about investing in this space, questions you should be asking yourself and questions you should be asking the promoter.

I think that really the only way to address it is through education and through kind of benevolent skepticism when presented with an opportunity to really think carefully as to whether this is somebody you would trust to watch your dog. Is it somebody you really want to loan your money to, give your money to, invest your money with.

MICHAEL FRISCH: And if I had any advice for the general public related to like where to trade cryptocurrencies, as Colleen said, you know, there's a new push for self regulation and standards that frankly I applaud. But there's a wide variety, a wide variation between some of the stronger firms with US connections. I don't want to single anybody, but you know, Gemini and Coin Base, those are based in the US with strong connections to the US, that are regulated lightly because they take fiat money. So basically you can wire US dollars into those exchanges.

And so they're required to do some amount of know your customer, KYC, some amount of monitoring for money laundering and other things. And so there's some standards go along with those light requirements. But there are other exchanges that don't take wires of actual money, where they only accept cryptocurrencies to trade on. They're not based in the US. They have very light US connections.

So these firms only require an email account, an email address and a password. And you know, you could be wiring tens or hundreds of thousands of your hard earned dollars to some exchange overseas. You have no idea who is behind it, what policies, what consumer protections they have. There's very little, if any, recourse for you if the exchange is hacked or if the owners steal your money.

So to me, getting defrauded by some promoter starting a new coin is a risk, but as significant a risk, I think, is sending your money to some exchange that you know very little about. So that's, again, customers should be very careful about which exchange they choose to do business with.

COLLEEN SULLIVAN: And I'd to highlight something Michael and Sarah Jane both said there, because I think it's interesting. Sarah Jane mentioned how you could get a freeze on a bank account. And Michael's talking about some of the international exchanges where they're, what we call, crypto to crypto, so there's no bank account relationship. So I always think of one exchange in particular.

And I'm not aware of any fraud or anything bad going on there at all, I just use them as an example. They're the largest crypto exchange in the world right now, Binance. They launched in July of 2017. They've just grown rapidly. But they're crypto to crypto only. So to the extent there was some theme, you know, maybe not great going on there, there's not a bank that the regulators regulate that you can lean on to stop that activity if there's a gap in regulation with respect to the exchange itself. And there's no bank account to freeze if there's bad activity because it's just crypto to crypto.

And I think from a regulatory, arbitrage kind of way of thinking Binance is interesting too because the founders were originally based in Hong Kong. And the SFC had some issues about what they were listing. And finance, just then, relocated to Tokyo. FSA had similar issues in Tokyo and Binance moved to Malta. So there's not much tying exchanges physically to the jurisdictions they're located in. A lot of these exchanges are online training programs or whatever you want to call them, are in the cloud. They're in AWS. It's not like they have necessarily headquarters in a physical building where people are coming in every day.

So the regulators have an incredibly tough job, I think, in this new environment because it's all so small right now. So when you look at the total market cap of crypto assets, it's $252 billion, I think, as of this morning. It's fallen quite a bit since the highs. Gold is $8 trillion. Our global equities markets are $79 trillion. But you also have a huge retail population exposed to highly volatile assets. So how do you find that right balance of consumer protection and not stifle innovation? That's a lot to think about.

You guys have the hard job.

MICHAEL FRISCH: Yeah, I mean, just to add on, when AMF Global collapsed, that was a highly regulated, you know, US-based entity. And the CFTC is proud that there was no actual end user customer that lost any money. The system worked there. And whereas I know in 2017, or maybe it was late 2016, Bitfinex, another one of the companies that I brought a case against was hacked. I think they lost about, at that time, $72 million worth of Bitcoin.

And what they did is they basically decided to socialize the losses across the traders and gave everybody a 30% haircut. Now, is that OK? Who do you go to if you're a customer and you don't like that? I mean, there's no rules that the CFTC or any federal regulator I'm aware of has to-- or standards to enforce that. So again, not only when you think about are they going to steal my money, but things can go wrong. If you're trading on a regulated exchange here in the US you have so many more protections. You have protections from your money in bankruptcy. You have protections from-- there's a whole reparations process at the CFTC if you get defrauded by your broker.

So there's so many-- there's so much more for you there to trade on.

DAVID HIRSCH: I think I would echo that. And one of the things that is a focus for the SEC as an agency is trying to bring folks into the light and get them into a compliance regulatory framework. So we will be able, hopefully, to deal with them in a more traditional manner, that there is more traditional set of disclosures, but also protections and recourse in the event of bad things happening. So it would be a more traditional model of how they operate.

And I wanted to echo something Joe Rotunda said on the last panel, which is we as an agency don't view blockchain or distributed ledger technology as an ill or a problem. It's a people issue. And so, you know, the SEC has a three part mission. One is to protect investors. Two is to facilitate fair and efficient markets. And three is to facilitate capital formation. And so there can be some conflict there where new technology is maybe really effective at helping to facilitate capital formation and that's part of our mission statement. We need to encourage that.

We just can't allow that to happen fully at the expense of protecting investors or having markets that are fair and efficient. And some of the unregulated exchanges, if there's no one there monitoring, if there are no rules standardized that they're all playing by, I mean, how are you as a investor or consumer sure that there isn't market manipulation going on? There isn't spoofing. There isn't previewing of your orders and trading ahead of what it is you want to do. There's just a lot more uncertainty when you're dealing with folks who are not compliant or not within a larger framework of regulatory compliance.

DUANE POZZA: Sarah Jane.

SARAH JANE HUGHES: So there is a gap filler, in part, coming down the road pretty fast. And that is the work of the uniform law commission in this space. The uniform law commission has approved and will soon have a second piece. But the first piece is prudential regulation of people who issue virtual currencies in a centralized way, or who offered to transact them or take custody of them on behalf of others. One of the beauties of virtual currencies, if you want to do it that way, is it can be a peer to peer transaction.

But many people don't do peer to peer transactions. They use someone else to do that work for them like many of us still use banks to do that work for us. Or people perhaps with less means and people who might be more susceptible to some of these scams use money transmitters, MoneyGram, Western Union, all kinds of people like that, check cashers and others. So the uniform law commission's uniform law that was approved last year will do prudential regulation of the same model, basically, as money transmitter regulation that has been in place for several decades in many places.

It's lighter, in some respects, than money transmitter regulation. But it will have some additional protections, such as protection from the creditors of the provider. If you they're holding your money, they have to hold your money as a liability. And they will have to be able to protect it in some way that they can satisfy the regulator with. Money transmitter's net worth requirements and capital adequacy requirements tend to be on the heavy side. We tried to lighten it up to allow people who are innovators to be able to begin their businesses, do some testing in the wild, without having all of the responsibilities and without the significant upfront cost of getting a full license.

We have an intermediate space between a full exemption from this ex coverage for people who are not just trading house money or using house money to test below $5,000. From $5,000 to $35,000, this new act will require that you tell the state you're there and follow some of the consumer protection and disclosure requirements. So if you're going to handle other money-- now Peter Van Valkenburg, with whom we worked on this project, once said something that others have said today about if it quacks like a money transmitter, it ought to be regulated like a money transmitter.

But not necessarily using exactly the older money transmitter models because the definitions don't work. There is no interim registration or sandbox kind of space so you can do some testing in the wild. And like the bit license, model which many of the states did not care for, or they just are jealous of New York, I'm not sure which, that one they won't certainly want me to say, but too bad, I already said it. The thing I think is though that process was used extraordinarily slow, there were only a handful of companies-- three, almost three years later, I think the announcement was June 24. But the license applications were due early August of 2015.

And we're talking about fewer than 15 companies that have received licenses.

COLLEEN SULLIVAN: Seven.

SARAH JANE HUGHES: Yeah.

COLLEEN SULLIVAN: And two trusts.

SARAH JANE HUGHES: Two trusts, right. I mean, it's a tiny number. And the two trusts, all of it seems to be going OK from what we can tell. But it is a very slow process. So if you file as a registrant under this law, you could continue to work until they told you weren't going to get a license from the state that was involved. The states, historically, have regulated non-depository providers of consumer financial services. And this is a way for them to continue in that role.

The states are often seen, sometimes accused, of being innovators or incubators in regulatory spaces that can be very valuable. Identify regulatory gaps that sometimes Congress has the wherewithal to address. Sometimes Congress doesn't. But I think it is really-- or they just don't have the appetite for it on the agenda that they have-- I think it's really important for a very strong web of collaboration with local, state, regulatory, and enforcement agencies, legislative bodies, and practitioners in financial advising, MNA, lawyers advising clients about partnerships.

And in Chicago, this huge FinTech industry that is coming here can be a very important player in a kind of important industry self-regulation that's worked pretty well in some other areas of the law and a market. And I'd like to think that that is a model that will be picked up. That will not solve all of these problems, but it will go very far as long as there continues to be robust enforcement a lot of education, aimed at different audiences.

DUANE POZZA: So we've talked a little bit around industry self-regulation. And in light of sort of the kind of hardcore frauds that we've been hearing about throughout the day, which is a challenge for anyone to deal with on the industry and the enforcement side, what is the sort of the practicalities of industry self-regulatory efforts in this space? And what role can industry play in either helping to identify frauds or helping law enforcement identify frauds? Or otherwise trying to get the fraud out of the space?

COLLEEN SULLIVAN: Yeah, so you know, I think why-- so in a new sort of asset class, in the new technology, I think where self-regulation is helpful with law enforcement is the initial participants in putting these standards and best practices forth are the ones actually in the space. So you take, again, for example, Gemini, they're operating a crypto spot exchange. And they've brought in NASDAQ to do market surveillance on the exchange. They've gone-- you know, so they see this gap. And they're implementing pieces from traditional exchanges that are regulated into their own marketplace.

And then their hope is to then take these standards of best practices and put them out there. But also as part of that effort, you've got trading firms like CMT that are collaborating with them. So then we can share what we're used to seeing in the marketplaces and what we're observing trading these marketplaces as an industry participant. So I think having that practical experience is part of the self-regulatory initiative in the early stages is important. With the hope then being that the regulators and these SROs are working together.

And I should clarify. The virtual community association that Gemini is working on is different than NFA and Finra. Those two SROs are mandated by Congress and receive funding from the government, and therefore they have more enforcement capability. The virtual community association will not be mandated by Congress any time soon, I would think. It's going to take a while to get there. But they will have their own sort of mechanisms within that structure to hopefully influence the behavior of the members that are part of that association.

Similar to the Token Alliance that Amy mentioned, the chamber has 160 different members. There are 300 plus participants in putting that together. Those are all industry participants. So it's just helpful, I think. I mean, I am in this industry 24/7 and I can barely keep up. So you have regulators who are doing nine million other things. I don't know how you even begin to stay on top of all of it. It's really challenging. And this technology, unlike-- to me, the internet was like a slow evolution compared to what we're seeing in the crypto, blockchain space. It's kind of incredible and exponential.

So I think that the industry helping participate in these early days, and I think the industry realizes it. Like the week, blockchain week, in New York, which was just six weeks ago, I went to four different self-regulatory meetings with people, four different groups, that are trying to put forth standards in different aspects of the industry. So I think the industry gets it. We have to start policing ourselves.

MICHAEL FRISCH: And I hope to see more referrals. I mean, the [INAUDIBLE] exchanges, like the CME and CBOT, many of the CFTC's enforcement actions start with a referral from an exchange. And the exchanges are in the best place to see whether wash trading, market manipulation, pump and dump schemes, or spoofing, or other bad practices are going on on their exchange. So I can't say that's not happening now. But I hope that it is something that will happen in the future.

COLLEEN SULLIVAN: Yeah. And that's a good thing to have in open dialogue with, like these groups that are putting together these best practices and standards coming in to meet with the FTC, the SEC, the CFTC, FinSEN and talking about how do we open that line of communication so we're sharing what we're seeing.

DUANE POZZA: And I'd actually like to broaden that conversation a bit, like what are the best ways to get complaints that enforcement can act on? I think there was even a suggestion in the previous panel that we should act before we even get a complaint based on how quickly these things are moving. Is that helpful to come from industry? Are consumer complaints very telling? Or are they sort of too late by the time we get them?

Like what are the ways that enforcement should or should gather information about this and figure out the biggest problems and go after them?

DAVID HIRSCH: So for us at the SEC, we have a very robust system where we take consumer industry expert, any complaints, it's called the tips, complaints, and referrals. So a lot of my investigations begin when someone comes in and gives me a TCR, tip, complaint, referral. And that would just be from anyone. So one of the reasons I like to be out in the public, like to be at these events speaking, is to request that anybody who is aware of things, doing research for yourself, if because of your position in the industry, if somebody gives you a hot tip that sounds too good to be true, please shoot me an email.

Please go to the SEC. Go to investor.gov. There's a link there where you can submit a complaint or a referral. But we get them from sister agencies, so Texas State securities board or other state regulators. We get them from criminal law enforcement agencies. We get them from the public. We get them from industry. But I think everybody who is interested in seeing a broader adoption of blockchain technology, or sees promise in this industry, agrees that it is going to be a quicker adoption and a smoother adoption with less fraud in the market.

And one of the ways to try and remove some of the fraud in the market is to notify regulators. Tell the cop on the beat there's a problem so that we can come in and try and clean it up.

SARAH JANE HUGHES: Were those that are moving really fast, that is a two day deal, that's never going to be a solution. But it just occurred to me throw out an idea that came to me some months ago and then I left it. And I thought about it again just listening to all of this, which is, I think that there could be some more focused community-delivered, not virtual-- not the virtual currency community, but communities and people who are counseling older individuals.

So in the state of Indiana and Massachusetts where we have homes, there are very robust counsels on aging that provide all kinds of services. I worry that vulnerable populations, people who don't speak English very well and are newly arrived, people who are at home a lot, vulnerable to the 15,000 telemarketing calls we all get every day but we're not there for, but they're there to answer the phone. They don't hear well. The English is sometimes accented [INAUDIBLE]. But I'm beginning to wonder if we shouldn't try to aim some education that people like that in churches who provide remarkable resource opportunities for certain kinds of people who might have some funds that they saved, they lost big savings in the deep recession.

And they're trying to get back to where they were financially. If we could think how to do something that would deliver at the local news level but way closer to the floor of the local news, I think we might suddenly provide people with that pause moment. Because Marie's-- her discussion of her research makes me think that what we have to do is make people not push the button to send the money, and that we have to find a more appropriate, fast response way, not to talk about specific companies, but to take something from your 60 point idea and figure out the facts that you guys have in the FPB or the BFCP has, whichever your politics are.

Because that's with the accents, I guess. The point here is we have to reach people before they push the button because for the most part, reaching them after they pushed the button on a fast moving fraud is no recovery.

MICHAEL FRISCH: And I agree with that. And to add one point is, look, I think banks, retail banks, have a role to play too. If you're an employee in a savings and loan in Omaha, and your client is a 70-year-old widower, and you see $13,000 wire to some cryptocurrency exchange in Bulgaria, then there should be a phone call, you know. Is this really what you're trying to do here?

And I think in this day and age, with the huge mega banks, and there's less of a one to one connection between bankers and their clients, I think some of that, that last line of defense has been weakened over time. Hopefully we can--

SARAH JANE HUGHES: So I thought we were supposed to learn that lesson from what happened to the government of Bangladesh. They had the $15 security system and I think the banks can do that but the outgoing wires are subject to a whole bunch of existing rules. And the question is, are the banks really doing this article 4A sales security procedure they're supposed to have and call the customer if it seems like an out of pattern deal, because the customer may say, yes. I authorized that transaction. Or the customer may say, as my late father and father-in-law both seemed to have had some of these problems, no, I don't remember that transaction.

And if I don't remember that transaction, I'm hoping the bank won't push the send button. But who knows?

DUANE POZZA: Sarah Jane raises the broader point of how do you reach consumers, especially when they're confronted with the sort of fear of missing out.

SARAH JANE HUGHES: Absolutely.

DUANE POZZA: What are the best ways to get them? I know the SEC did this stop and pause moment with the Howie coin, maybe you could talk about that, and other sort of strategies that we have to educate consumers who are still even trying to figure out, as we are today, the language around this and the terms.

DAVID HIRSCH: Sure. And another disclaimer, I had no involvement in this and really only found out it was happening when it went live on the web. But the SEC issued something that it called the Howie coin. And that calls back to the Howie test that I referred to when we started speaking today. And they said that the Howie coin-- they issued a white paper. And they said Howie coin is this great new investment opportunity. It could revolutionize the travel industry with the benefits of decentralization and blockchain.

Like they made their own word salad. They had pictures of people who don't actually work for the SEC or aren't associated with any offering in their offering. They had it very much like a scam white paper. And that if you click, I'm interested-- and it promised outlandish returns and did everything you would expect for a white paper that was ill-intended or malicious, and if you click I'm interested to buy, it would automatically redirect you to investor.gov and would give you education about here are some of the things you should have been looking for in the white paper that should have clued you in that this is potentially a fraud or a scam.

And you should be skeptical go forward when you see things like this. I thought it was very clever, very creative, a good way to really put into practice the things that our chairman has been saying and that we as an agency have been saying for quite some time about the importance of investor education and investor awareness, and a healthy degree of skepticism when talking about investing your money.

SARAH JANE HUGHES: Because ultimately, turning the spigot of money on is the only way this is going to get solved. And that is clearly a collaborative venture that's going to go on for a long time. But I want you to do something for the audience just in case, and that is, we've talked about the Howie test. But we haven't told you what's in the Howie test. So, Howie test, please.

DAVID HIRSCH: Sure. The Howie test is, in analyzing whether something is an investment contract, and thus the equivalent of a security and the sort of thing that the SEC regulates, you got to ask yourself, is it an investment of money with the expectation of profits, in a common enterprise, based on the efforts of a third party? So Howie was an orange grove.

And basically, they said, you can invest here. You could buy part of the orange grove. And don't worry about it. We will-- you don't even have to live anywhere close to it. We will grow the trees. We will harvest the origins. We will take them to market. We will sell the oranges. You just sit back and let the money roll in. And the Supreme Court said that is effectively a security investment. That's an investment contract. It should be regulated like a security. If you're going to offer that, you need to register with the securities and exchange commission unless you qualify for an exemption.

And the same rule has been applied to pay phones. Some of the younger people in the audience, I can tell you what pay phones are later. It's been applied to lots of different things. It's a very flexible analysis that says, because people we're working up against, in some cases, are also clever. They're trying to find ways to engineer how they describe what they're offering around the plain language of the regulations. And the courts have said, that's not good enough.

It's not the words you use. It's the substance of what it is you are doing. And so Howie is a very flexible test. And it's been applied in the same way to orange groves, to pay phones, and now to digital tokens. If you're offering something with the idea that the investor, the purchaser, is going to profit as a result of something you're going to one day build, or that you're in the process of building, or that you're going to make more successful and that's going to generate more money for the investor, you may well be offering an investment contract. And that is likely going to be regulated by us unless you can establish why you qualify for an exemption.

DUANE POZZA: So we have two minutes left. And my last question, it's a speed round, then. We often, as enforcement agencies regulators are always balancing enforcement with protecting consumers with innovation in a very innovative space. And we're always mindful of that. This is an area where we've heard of a lot of consumer harm and a lot of fraud. At the same time, it is a rapidly growing innovative space. Do you have concerns about a balance between enforcement and pro-consumer innervation here?

And what is the best way for-- and I'm looking at Colleen to answer this question first, for enforcement to go about protecting consumers while keeping open pro-consumer innovation?

COLLEEN SULLIVAN: So I don't think I can really speak to the enforcement side. But what I will share is three weeks ago I was part of the blockchain impact summit at the United Nations. And I was part of that financial inclusion working group. And in my group, we had former refugees, very interesting group. And one of the things that I brought up was digital identity and the potential around that.

So you know, if a refugee is in a place where there's an unstable government, well, starving in a place where there's an unstable government to the extent that they have some type of the device that can hook up to the internet, where they can have a digital identity, a digital wallet. They have assets in the fiat of that country. They can convert those assets into some type of crypto asset, held on their digital wallet, and they have an identity, there's value in knowing that if you have to leave some place-- these are things I think sometimes we take for granted here.

But if you have to leave that place and go somewhere else, no one can take that from you. You can also start over and people will know maybe you were a doctor in the place that you left. And now you can start your profession where you've gone. So I tend to think about that in terms of doing our best to not stifle innovation. There's also regulatory arbitrage that we need to worry about. But consumer protection is so critical. And the stories that were shared in the prior are, frankly, heartbreaking.

So I don't have the answers. I just know that striking that balance is a really, really tricky thing in this space.

SARAH JANE HUGHES: So I'm going to say something completely different. But I absolutely agree with Colleen first. And the thing I think that we need is better data. And if you went, and I did, the Consumer Financial Protection Bureau has a great complaint database that you can look at. But in this particular arena, it lumps remittance payments, wire transfers, and virtual currency problems into one category.

And the most recent search I did preparing for this panel showed-- this was last week-- approximately 6,800 complaints. But when you read them, many of them, the person being-- the entity, rather, being complained about was a bank. So that is harder when you get down to the more granular level and you look at what the complaint actually is about, it may or may not have anything to do with virtual currency, to the degree that agencies can keep better-- keep and then publish better data.

They can enable many of the people in this room and groups that are working to have a better idea of where these problems are actually arising, which will allow a lighter hand for the people who are registering and trying hard to comply with the law and provide a better flashlight being flashed on the persons who are not doing this in a way that is above board.

DUANE POZZA: Great. We're out of time. So thanks to our panel.

[APPLAUSE]

And now for closing remarks is Todd Kossow, the head of our Chicago office.

TODD KOSSOW: Thanks, Duane. And thanks to our last panel. So as Duane said, I'm Todd Kossow. And I'm the director of the Federal Trade Commission's Midwest region office here in Chicago. Well, it's certainly been an interesting afternoon. I want to thank all of you for joining us today, both in the room and on the webcast. And thank you, again, to all of our exceptional panelists and all three panels. We certainly covered a lot of ground this afternoon in a short period of time.

So we were very pleased to be able to start the workshop today with remarks from the FTC's new director of the Bureau of Consumer Protection, Andrew Smith. We're really glad that Andrew was able to come out from Washington to join us for this event. And as Andrew said earlier, we're here today to advance the conversation about understanding and effectively combating cryptocurrency scams. And I think our three panels today helped us do just that.

In the interest of getting you all on your way, I wanted to highlight just a few takeaways from today's workshop. As we heard from our first panel, the cryptocurrency landscape is rapidly changing. We're seeing an ever increasing number of cryptocurrencies, and an expansion in the way consumers can use, buy, and otherwise engage with these cryptocurrencies. Our first set of panelists talked about the technology's potential, but also about the perils consumers face from the often misleading and confusing information that they need to digest in this marketplace.

Our second set of panelists told us about the various frauds that we're seeing in the cryptocurrency marketplace. From cryptojacking to deceptive investment opportunities to sham ICOs, there's no shortage of ploys that consumers need to be aware of and look out for. In many ways, these are the same old scams that simply are taking advantage of new technology, with some added challenges thrown in. These scams can sometimes be difficult to detect and our panelists talked about how consumers can better spot them and protect themselves.

Our third panel helped us take stock of where we are and where we can go from here in terms of preventing cryptocurrency scams. Our friends from the CFTC and the SEC spoke about the complementary roles their agencies play alongside the FTC, state authorities and others in monitoring the cryptocurrency space. And we did learn about the Howie test this afternoon.

Coordination is important, and we're all committed to working together to advance an effective law enforcement approach. And in addition to robust enforcement strategies, as Sarah mentioned, consumer and business education in this area is essential. Providing practical advice to consumers attempting to navigate the cryptocurrency marketplace can help minimize the spread of scams.

So as Andrew said earlier, the FTC will remain an active enforcer of consumer protection laws as new technologies emerge or existing ones develop. And we'll pair that with timely consumer education. Of course, for us to stay on top of how developments in technology are affecting consumers, it's critical for us to hear from them directly. If you or someone you know experiences a cryptocurrency scam, please file a complaint with the FTC at ftc.gov [INAUDIBLE].

Finally and importantly for all the lawyers in the room, particularly those who need to report their CLE in just a couple of days, I'll remind those of you who are seeking Illinois CLE to pick up your attendance certificate from the registration table. And also please grab an evaluation and fill it out and submit if for us there. For those listening via the webcast, you can contact us at midwestregion@ftc.gov, midwestregion@ftc.gov to receive your CLE certificate of attendance.

Again, I'd like to thank the terrific staff at the FTC who put together today's workshop. And a big thank you to DePaul University for hosting. Thank you all for coming.

[APPLAUSE]