Barefoot Innovation Podcast: Ari Redbord, Global Head of Policy at TRM Labs, Carole House, CEO. Penumbra Strategies, Matt Van Buskirk, co-CEO, Regulatory, Hummingbird

***Note that transcripts may sometimes contain errors and that transcript timing notations do not match the posted podcast**

Jo Ann Barefoot: Hey, everybody. I am so glad that we are assembled to record part two of our podcast on fighting financial crime. I have the same incredible guests that we had in part one. We have Ari Redbord, Global Head of Policy at TRM Labs. We have Carole House, CEO of Penumbra Strategies, and also she is a Distinguished Senior Fellow at ACAMS. And we have Matt Van Buskirk, co-CEO for Regulatory at Hummingbird. We will link in the show notes to part one. Everyone should go back and listen to it. I don't think we've ever done a show before where in the middle of the show I said we have to come back and keep going. And then it took us longer than we thought we would need to reassemble. But in part one, we talked about the importance and the difficulty, but still the do-ability of making a dent in the growth of financial crime.

And what I want to do in part two is really dig deeper into the collective wisdom of this group to think about what really needs to be done, what can we do? Let's switch to action mode and problem-solving mode in a field where a lot of people spend their time talking just about how many problems they are and how huge they are. So before we turn to the solution topic though, I do hope everyone listening will listen to part one if you haven't. But before we jump into the next part, let's just recap a couple of thoughts on the scope, scale, and frankly, terrifying nature of what's going on in financial crime. So just give me your top-of-the-head thinking on something you want to be sure the audience is keeping in mind as they listen to the rest of this show. Ari, do you want to start?

Ari Redbord: Yeah, no, happy to. And thanks again for reconvening or bringing the band back together, Jo Ann. I think it's an awesome group and also really close friends. So I love these conversations. I guess a couple things are top of mind for me right now when it comes to sort of the problem set. The first is AI and AI is transformative technology, but the reality is that AI is supercharging money laundering, illicit finance and financial crime. We basically have seen bad actors leverage AI the same way we all do, lawful users to move faster. So we're seeing scam activity done at scale. You don't need scammers on the other end of a line anymore. You can have agentic agents who are sending these sort of spam scam text messages, email, social media engagement at the click of a button. Hundreds, thousands, millions. We've seen ransomware groups use AI agents to deploy malware.

We've seen scammers use deepfake technology and other types of technology to sort of really scale. There was a world in which scams and fraud were a series of phishing attacks and broken English. Today, it's perfectly tailored to individual users. So I'd say that's the first sort of thing that we're tracking really closely and

looking forward to getting into solutions there. And the other is really, obviously, I'm very focused on the digital assets ecosystem. We saw about 158 billion in illicit activity last year within the crypto ecosystem. That is a record setting year.

Still a relatively small percent of overall illicit activity, but what we're starting to see is bad actors, particularly nation state actors, really leverage infrastructure rather than, these are not just one-off payments anymore that we're tracking and tracing. This is nation state actors, IRGC in Iran, for example, using cryptocurrency exchanges to move billions of dollars. It's Venezuela, it's cyber attacks at the speed of the internet by North Korea stealing billions of dollars. So I'd say those are sort of the two big things right now is bad actors using crypto infrastructure really at scale for the first time and obviously AI just over everything.

Jo Ann Barefoot: Yeah, yeah. Carole, what do you want to point to?

Carole House: Well, of course, Ari's incisive as always. The speed and scale of the evolution of the tech, the adaptation of these technologies for illicit purposes by these transnational organized crime groups remain front and foremost here. They're front of mind and really a core issue that we have to figure out how to increase the pace. So I think that's an underlying issue that really helps to highlight some of the bigger problem sets that we have. We still have a major problem of speed and scale of enforcement, which I know isn't necessarily the most popular view across the industry, but the idea that enforcement approaches often take actions on a fast timeline like citing activity from four years ago, but in many cases are in fact citing activity from a decade ago. That is not a pace that is an effective deterrent. It's not an effective disruptor.

This is not working and it's definitely not working when seeing the 1,300% increase in deep fake fueled fraud that I think Pindrop just dropped that assessment. But there've been many other assessments about the 100,000% fold increase in fraud and other AI illicit activities in cyber crime as well as financial crime that's occurring. But it underscores this bigger problem that we've had even before we had the generative AI uptick in all of this, which is that we are not keeping pace with enforcement and application across the industry. And even if you have policy that applies, if you're not enforcing it and not implementing it, then it ultimately ends up being feckless in the first place. I think some other underlying issues, we've not really addressed the core building blocks and I guess that'll lead into some of the solutions that we need to get to.

But this absence of strategic thinking at looking at, what are the core underlying causes of a lot of these things? The complete absence of effective digital identity infrastructure continues to be one of my many high horses. It's my highest horse, in fact that I like jumping on. But this problem has reared its head, certainly in cybercrime, definitely in fraud. Obviously, identity is the major vector of compromise that's occurring there. But now ultimately with agentic AI, without effective digital identity, you are just continuing to systematically build

in pro-cyclicality and programmability and scale and delegating authorities into a world where we do not have sufficient trust across the digital ecosystem.

So these issues about the speed, scale, and sophistication of the technologies being exploited very quickly by bad actors who are looking for those seams. And we're not even keeping pace tactically after the fact, right of boom on the enforcement side. And we're certainly not looking at the root causes and investing in those. So I think those are my biggest concerns. Also, I'll say that I do think that prioritization and dismantling of a lot of critical rules and enforcement apparati are some other concerns that I'm worried about right now. A big focus on cost and not enough work thinking about the efficacy and the benefits of an AML framework.

Jo Ann Barefoot: Yeah. Matt, what do you want to add?

Matt Van Buskir...: I think some of the data points I would be citing here or maybe repeating from our first episode. A couple of things I remember coming out from a conference in London that I mentioned before was that the explosion in AI is making it cost-effective for scammers to go after people who maybe their whole net worth is only $50 now, where previously they were trying to target wealthy retirees to get more bang for their buck. I also heard recently that countries like Finland previously had no real problems with fraud because the language was not commonly spoken and fraudsters were mostly going after English-speaking countries, but suddenly you have an entire country that is having to deal with a problem of scams coming in in perfectly written finish without any cultural antibodies to not responding to these types of messages and expand that across the entire planet, you're starting to think or see.

If scams exceeded narcotics as some estimates have shown last year as the largest category of criminal activity, I feel like it's only a drop in the bucket compared to what it could be as these things keep getting accelerated through adoption of all the technologies. So like it or not, this is an arms race. We can't continue to defend ourselves the way we have been when the bad guys out there are adopting the bleeding edge constantly.

Jo Ann Barefoot: Yeah. Matt, you might have said this in the prior show, but I think you've got a statistic that the North Korean missile program is mostly funded by scams against the West, is that accurate?

Matt Van Buskir...: Yeah.

Jo Ann Barefoot: And also something you said to me that really struck me was that if financial crime was a country, it would be a member of the G7. And we're acting like somehow if we just keep doing what we do, but do it a little better or a little more or something, we're going to solve these problems. And as you said, Carole, we are not on a track to solve them. To the contrary, it's all getting worse

and we're trying to combat these problems with tools that don't scale and don't move quickly and so on.

So what we want to do in today's show is, let's pretend for a moment that you all have been made the czars of solving financial crime by whatever powers that be in the US, internationally. Somebody has said to you, "Come up with the blueprint for actually turning the tide on this." And we know we're not going to eliminate at all. We'll talk later about what good looks like, what success looks like, but right now, the people driving this, including these geopolitical players who are really making a nexus between this crime and national security issues all over the world, we really want to think about what is the ecosystem of change that needs to happen and go from there. So what are the most important things that need to be done? And then we're going to talk about what's preventing them being done and what to do about that. Jump in.

Matt Van Buskir...: I guess I can start here. I got an invite to a Council of Europe event in Brussels about three weeks ago, and the initiative that they're exploring there was really interesting. Basically, they're trying to create a common minimum data standard for suspicious activity reporting across Europe. And in the initial briefing they pointed out an example which saying, "If you're a financial institution filing in Europe and you're filing in multiple countries, because you operate in multiple countries, you know that a particular fraud ring or something that you're reporting on cuts across all these jurisdictions. But if you file in France and you file in Germany, France and Germany can't tell that it's the same actors even on the same activity being reported because they have different data standards." And the FIUs were sort of saying, "We need to be able to trace this activity without having to do a whole bunch of data reformatting in Excel literally every time."

So basically the structure of how we've imposed regulations globally is actually imposing, well, structural challenges going around the bad guy or catching the bad guys. They're able to run rings around us. So a couple of things stood out to me about it. It was led by the FIUs. They were coming to the Council of Europe and the European Union and saying like, "Hey, we need to figure out something to do here. They're coming up with a technical approach themselves." This was sort of a learning event across the industry where they were presenting their initial thoughts to get feedback across the industry from a wide variety of different types of financial institutions, from traditional banks to crypto to gaming companies, all that kind of thing. And it was two days workshops basically. And there was a ton of feedback and one of the challenges I saw was towards the end of it, one of the financial institutions were raising their hands and really trying to emphasize how expensive everything was going to be whenever they were changing these efforts.

And one of the FIU representatives got up and said, "Well, we kind of have to do this if we actually want to do something about financial crime." And it really cut back to the core theme I think we've experienced here, which is the fight against

financial crime for 40, 50 years now has really been treated as a compliance exercise and it's not. It's a conflict. We need to stop treating it like compliance and we need to be ensuring our regulatory bodies are holding people to a standard that is not how good they are in executing paperwork, but how effective they are in getting information into law enforcement. And I hope to see we can't fight global crime locally, and that's what we've been doing, and the more we have this fragmentation around the world of all sorts of different reporting standards and such. It'll be structurally impossible for us to make a real difference. So the EU initiative is really exciting and I hope to see more of those happening that are more global in nature as well.

Ari Redbord: Yeah, happy to jump in here. I mean, I love Matt's take and I remember from the last segment also I thought he beautifully articulated this idea that this is not a compliance issue, this is a national and global security issue and we should start treating it that way. Building on that a bit, if I had that magic wand, Jo Ann, I'd really start with public-private partnership and as I just said that, everyone's eyes glazed over in your audience, because that is the cop-out answer whenever you have a recommendation for anything. But what I want to talk about is not, I think how we've always conceived public-private partnerships, but we really need to reimagine them. It's not a bunch of people sitting around the table iterating on standards and best practices. It's real-time information sharing, interdiction, seizure, prosecution and offensive cyber type activity.

We live in this really interesting moment in human history where the private sector holds all of the data and the public sector has all of the authorities, and we really need to give the private sector some of those authorities and we need to make sure that the public sector has access to all of that information. I talked, I think in our last session about The Beacon Network, which is a real-time information sharing and interdiction network for crypto. I think we need to kind of expand that. I think there's all kinds of conversations on letters of marque that is happening on Capitol Hill.

I'm a very big proponent of that type of activity where the private sector has authorities to actually proactively go after and seize funds. Carole is smiling and I'm never sure whether that means she agrees with me or is excited to disagree with me, so I'm going to let her jump in here. But when I think about public-private partnership, public-private information sharing, to me it's about disruption. It's not about a bunch of people sort of sharing ideas around a table, which I think is kind of sadly how really public-private partnerships have looked in the past.

Jo Ann Barefoot: Yeah, thank you.

Carole House: Yeah, so I was actually going to bring up the letters of marque debate because it's such a big area of focus and it's always something that comes up, at least-

Ari Redbord: Is there a debate? I just think it's an amazing idea pretty non-controversially, but I'm sure there are people who disagree with that. I'm very leaning into this.

Jo Ann Barefoot: For the audience's benefit, explain what it is.

Ari Redbord: Absolutely. Carole, you want to go for it?

Carole House: Sure. So there's my cheeky answer, which is cyberspace piracy. But okay, so back into actually what it was. Back when pirates were very, it was a very real problem and basically the US Navy just didn't have the ability, the resources to be able to go and counter the amount of piracy that was hurting Americans and commerce. We issued letters of marque to privateers, so basically state sponsored pirates, like lowercase P pirates to go after the capital P pirates to go after the bad guys that were hurting American commerce. Generally, that ended and went out of vogue because it got exploited in the end, but there were certainly successful examples of it, but when an authority like that is not properly overseen, which was especially difficult at that time, I would say there's a reason why that went out of style and then literally went out of style in the sense that privateering is now a part of the Treaty of Paris Accords, which I know the US has not directly acceded to, but generally has adopted those norms as a practice to not support privateering.

So there's some really interesting questions around international norms, which certainly I will say that even now in the geopolitical context has been, there's certainly a lot more interest in discounting certain existing norms, especially if we feel that it's in us interest. So I understand why it's top of mind and frankly it's been, I saw it as a point of discussion on the Hill, both under Trump 1.0 and in the Biden administration and otherwise. It's one of those things that comes up as a point of discussion, and it's becoming very meaningfully fully mentioned here because especially when law enforcement timelines are like what I mentioned and the fact that as things get more and more digitized, there's lots of very valuable information and now where data is also the asset of value with digital assets, then you get into where it had traditionally been, in my experience, sort of siloed into cyber security discussions and debates around hack back debates. It's now being discussed in crypto recovery to try to get back assets like either sometimes discussed in ransomware ransoms, but for the most part it's more like in crypto heists, thefts, and frauds.

So I have my own feelings about whether or not you need a letter of marque. I think ultimately what I do completely agree on is that there needs to be a scaled actual strategy and approach building the technical policy rails and political will to scale asset recovery capabilities, including in partnership with industry. I don't actually think that you need letters of marque to do that. I think that the US government has plenty of existing authorities including contracting capabilities and others to be able to do it without letters of marque, but either way, I'm function over form. Whatever it is, it needs to be a public-private partnership to enable that asset recovery and then specific policy makers can discuss and

debate the pros and cons of very specific forms to be able to do that. So either way, I'm very much on board with the need to scale asset recovery capabilities in partnership with industry, whether it's through letters of marque or through something else, but it was really neat to see it bridge from hard cyber conversations into the cryptocurrency world. So it's a neat point of debate.

Matt Van Buskir...: I think that's a theme that we should be emphasizing here, that a lot of the cyber world is much further ahead than the financial crime world in the realities of a lot of these threats that we've been facing. And they actually have implemented solutions and new types of public-private partnerships that, I mean, they obviously could be improved upon, but compared to what we have in financial crime, they're much better. So we're not reinventing the wheel here. There are methodologies we could embrace.

Carole House: Yeah, I totally agree. This was something that even since 2018, certainly as a regulator, we were encouraging industry, and I wish that the government had also picked up the torch sooner, but I think that we can now on exactly the initiative that Matt was talking about that's happening in Europe. This issue around there is no, in cyber you have things called STIX and TAXII, the standards for sharing of cyber threat indicators and information, because we learned this lesson that when criminals are exploiting your globally connected infrastructure at the speed of the internet, that you need to be able to share in an instantaneous machine-readable way information and indicators around what's happening on the offense and then how to defend against it. We haven't done that with illicit finance. We have tons of financial information standards and there's tons of standards on literally ERC-20 tokens.

This is something that would be perfect, perfectly positioned for cryptocurrency, but also just generally for illicit finance, we should have that standard and that should be feeding into exactly what the structured data fields are that law enforcement is asking for in response to subpoena requests and that agencies like FinCEN are leveraging. There are some really brilliant minds who have been talking on this, like Natalie Loebner has commented on this for a long time, and I think she's totally right. This issue of us not investing in those underlying building blocks of fixing the data problem, which will enhance the, at least getting actionable information into the hands of the right actor.

Then if the actor doesn't act, enter enforcement or enter other levers of influence. If the first step has to be that partnership that Ari was really emphasizing of getting actionable information into the hands of the right actor, and then if they don't act, figure out the right incentive, carrot or stick, to make them act. And that's where you think about authorities as well as other positive incentives and including things like liability protections and insurance, et cetera. That kind of mapping of thinking about what a strategy looks like in the near term, the nearest term is standing up those partnerships, finding those who are willing to act, leveraging that willingness to sit on the desk of industry, building those standards around data that we know very largely, there's the Global

Signals Exchange that's doing some of that work on technical information. We do this for the NCMEC, we can do this for illicit finance.

Jo Ann Barefoot: I have a million questions, but let me encourage you to just keep going. What else is most important that we haven't touched yet?

Ari Redbord: Matt, one sort of interesting thing is the distinction that you made between sort of the cyber space and the financial crime space, and I tend to sort of maybe just loop them together in some ways, right or wrong. When I think about cyber crime, it always involves money, either laundering funds or stealing them, essentially. These pig butchering scam compounds, 30 billion last year. That's probably 85% higher based on under reporting. I think of that as an interesting mix between, there's, to Carole's point, stealing funds at the speed of the internet, but having sort of a really close cyber nexus. I wonder to what extent there is too much of a silos around how we're thinking about cyber and how we're thinking about financial crime. And I know Jo Ann is the host here, but when you said that, it sort of struck me as like, "Hey, is that actually something we could be doing better?" And the answer is quite frankly, I don't know. I just tend to loop them in and talk about them only almost as one problem a lot of times.

Matt Van Buskir...: Yeah, I think the explosion in AI technologies, all these things, increasingly everything is becoming cyber in some way or another. But I mean, we mentioned in our last recording you were giving the example in Las Vegas of the origin of the FBI being the fact that we had cars able to drive across state borders, so we needed to have a law enforcement body able to fight crime across state borders. Our whole anti-money laundering architecture, financial crime architecture is still psychologically grounded in the '70s, and it is all cyber. Everything that's being done electronically now. If you are a multinational criminal organization, you probably are getting cash through drug proceeds and such, but your goal is to convert that cash into electronic funds that you can use to do other things. So it is, I think you're completely right, we need to be, break all the silos basically would be my number one recommendation for fixing this type of thing.

Jo Ann Barefoot: And that is, it's not just between illicit finance and cyber, but I think it's also within illicit finance. We have these very siloed legal frameworks, government bodies, activities inside a financial company for doing AML work versus fraud versus, so there's maybe we talked about in this for the first show, but there's fraud that if you're a bank that you've got to pay for if you don't catch it. But then there are scams that the customer's going to have to pay for because they've chosen to send their money to someone they shouldn't. Those are different categories, different people are watching over them, and they've got different compliance requirements around them.

AML has dominated for so long as a cost center and activity for the banks where the bank doesn't have much of an incentive to focus on that other than the

compliance side risk of it and compliance and enforcement. Fraud, they do have a self-interest in trying to save their own money. Scams, they're concerned, but they're not on the hook for it. So I just think, but as you're saying, they're increasingly blending together. The same people who are doing frauds and scams are laundering the money and the cyber, as you say, is a common denominator. So I don't know what to do about that, but I think we somehow have to connect this ecosystem in a different way. Go ahead, Carole.

Carole House: Yeah, I-

Matt Van Buskir...: I was going to say-

Carole House: Yeah, no, go ahead, Matt, because I'm sure that yours is right on that.

Matt Van Buskir...: Well, I was about to redirect it to you actually, Carole. I feel like my number one thing is break the silos, but I think I would also say the other biggest thing is identity.

Jo Ann Barefoot: Yeah.

Carole House: Yes. It's so true. There's so many interesting issues, and I think that especially in the current context of that in the US, what you're seeing is an emphasis on enforcement and new regulation is not what's going to happen for the next few years. So even though I think that mapping important regulatory controls is necessary, understanding the present reality is also critical. So thinking about what the near-term, mid-term, and long-term solutions and initiatives are, but first requires mapping, what are the problems? And you guys have pointed to several of the core problems. We do not have the trust tech infrastructure to really believe in a verified way who is in fact, on the other side of this transaction, selfie and liveness check and voice-based identification is no longer something that can be trustworthy. Sam Altman said that a year or two ago, highlighted that the state of AI is just at this point. There still are measures that can be put in place to try to defend against deepfake-fueled fraud, but the reality is that the tech is just going to continue to evolve and get more sophisticated.

So the reality is that we need to be looking at cryptographic-based identity solutions and actually promoting and supporting their adoption. Like some of the counter-fraud measures that we had put in the cyber EO at the end of the last administration that unfortunately were rescinded in whole. I hope that they reissue them all. It's part of a broader counter-fraud, like as an appropriately calibrated counter-fraud strategy and approach in a more strategic and cohesive way. That would be fine and good. And it's something that requires partnership with industry providers. TSA is doing some stuff right now about implementing work with digital identity providers through mobile driver's licenses. I think that there's some real investment that needs to get placed in on that front. And there's implications there for KYC, utility sandbox and experimentation.

But the near term efforts that can create the operational space for the longer problems are things like investing in this data, in re-hiring people and helping to support their scaled, iterative... Enforcement should be early and often across the ecosystem. It should, because if you have a groundbreaking, like record-breaking, huge enforcement penalty, that also means that we allowed it to become a record-breaking enforcement problem. That's not actually a good news story, and we shouldn't view it that way. We should view enforcement as a purpose of shaping a sector and not breaking it. So I think that there's efforts on that front that need to be invested in and focusing on, helping the people that exist there, scaling the ability to do enforcement, using that data, leaning on industry, but then also looking at efficacy. We have not done the work to assess and defend the efficacy of the AML framework.

Treasury has not done that work. Even the RFIs that came out from the agencies, while important to finally get real benchmarks for cost, did not ask the meaningful questions that were needed for the efficacy of AML, nor is there really a mapping and understanding of how AML controls are necessary for things like credit and civil litigation and taxes and revenue. There's a bigger connective tissue of these ecosystems. And in cyber, we see this because financial institutions love to point to, "Well, it's the tech infrastructure's problems. That's where we need to be pointing, because finance is regulated." We're not regulating for KYC purposes like domain web hosting services and other things. But there was a KYC for Infrastructure as a service EO that was issued by Trump 1.0 and then upheld by Biden, but it never got issued because there's huge tensions across industry as well as even inside of the US government on whether we want to put in place KYC frameworks that industry claim don't work even in finance, why would we want to impose that on more sensitive information activity?

These tensions need to be resolved, but those are going to be longer term problems of... So I think in the near term, thinking about how we actually measure efficacy of AML, which can feed better use of things like AI to detect it, and then those near-term efforts focusing on data and creating sandbox frameworks so that we can stop having to continue to circle in this, "We don't allow innovation in AML." Even though I think we do, but fine, publish some sandbox frameworks I think would be good.

Ari Redbord: Hey, Carole, real quick. So again, like Jo Ann, I'm not trying to steal your job, I promise here.

Jo Ann Barefoot: No, no, [inaudible 00:32:25].

Ari Redbord: We have responded at TRM to a number of these RFIs on BSA modernization across a couple of different administrations now. It's obviously something that FinCEN has been thinking about for some time, since you were there, quite frankly, and I actually think a lot of the questions are the right questions. What are the controls that you could in place? What are the tooling that can be used?

What is the technology that's out there? Do you have any inside baseball on where that is? And then I think one thing that's cool, I mean, Secretary Bessent has made some really helpful statements over the course of his time at Treasury on a risk-based approach, not a checkbox regime, thinking about using technology, AI, et cetera. Do you have inside baseball? And obviously it's going to take the Hill as well, and this is kind of a Herculean task, so maybe is it just like, this is too hard, but what's your take there?

Carole House: Yeah, I think the biggest problem that we have is that metrics on effectiveness of AML are hard, are really, really hard. And we haven't put the best thinking on economists and national security benefit and mapping with an overlap of regulatory frameworks into thinking about it. So even though I do agree that there's been certainly a lot of emphasis on trying to reduce cost, that's a part of improving efficiency. Haven't seen a ton on improving effectiveness besides wanting to integrate emerging technologies. Which, you're right, over the past decade that's been a talking point at Treasury. But actually making where the rubber meets the road is where I think the tangible problems and challenges have been, and mostly they've been around fact that we haven't done those underlying issues that will help to allow for that vision to be accomplished.

So it's not that the vision is entirely wrong, it's that I don't think that there's an understanding of the root cause analysis that if you don't fix the data problem, if you don't understand how these things intersect with even a national security community and the fact that law enforcement, do they even carry and capture any metrics just generally? And this isn't a problem for just law enforcement. Agencies, if you look at most of their assessments of efficacy, they're pointing to numbers of alerts that are issued, not actual reduction of risk, and this problem that we have on people that want outcomes-based enforcement approaches.

That's good, I like risk-based approaches. I've also never really seen an architecture for, and here's how you actually accomplish that at scale. Here's how you scale every examiner's ability to create a bespoke outcomes-oriented exam every single time that they go in and conduct an examination. It's the rubber meets the road problem. It's that translation that requires a really strategic approach to it. I hope that that's what will come out of a lot of these RFIs. This has been the problem that I think has been missing from a lot of the work over the past decade.

Matt Van Buskir...: Everyone familiar with the Santa Fe Institute and the concept of the study of complexity as a science?

Jo Ann Barefoot: I am.

Matt Van Buskir...: It's an interesting model. The kind of core concept that, without getting into the whole history, there's a book about them that's just called Complexity. And it was basically a bunch of Manhattan Project scientists who came together post Manhattan Project, and they realized that biologists talking to a physicist, talking

to an early economist or whatever, that the cross field population or propagation of thinking was causing inspirations in their own field just by hearing something from some other field. So that created the Santa Fe Institute. They are basically focused on the study of complex systems, which could be biological, how people interact, all that kind of stuff. The core thesis that they have though is just saying that a lot of the ways we as humans think, and then also the way we enact policy is we sort of try to simplify systems down to something that we can kind of model in our minds.

The solutions to this are simplifying them does not work, they're inherently complex, multivariate. Tweaking one thing here and there won't work. We need to be having a fundamental top-down reinvention of it. The kind of cool thing about it though is the advent of large language models and AI capabilities suddenly let us do a lot more of this sort of population level simulation of these types of things. But I think, Carole, to your point, the solution to this really would be something like the Santa Fe Institute or someone out there going and doing the research and coming up with, in my mind, a real solution to this thing is a much more tech enabled government with a lot more free flow of information going in real time back and forth. There's a lot of ways that could be hijacked for nefarious purposes. You don't want to have the government having unfettered access to everyone's financial activity.

So we've seen China go down a path of social credit scores and high level monitoring of everyone's personal lives. I think that we need to come up with a Western democratic alternative to that type of thing, which is acknowledging that we don't want our government to be hamstrung by excessive bureaucracy and paperwork and all these other things structurally slowing them down. We want them to have the ability to move lightning fast when it's needed, but you also need to build in the controls and structures and such to prevent that from being abused and have high transparency.

So I mean, if we really want to solve this problem, I think that we need to sort of stop hiding our heads in the sand and sort of waving our hands around and saying, "Now we're doing X, Y, and Z things that we believe will achieve a result." And actually find a bunch of funding to put together and commission real research on the costs, the impacts, the burdens, the ways things could be abused. And Ari, to your point, this will require Congress. We need to have a next generation overhaul of financial crime laws, but we all know Congress is not going to figure this out in a vacuum. They need to be given a credible path to follow, and I think that's where the community we're collectively building through all of our networks here and what AIR is doing is going to be vitally important.

Carole House: Yeah, I think that that same thinking is basically where the DOD Office of Net Assessment came from, this concept, but only seen in DOD and Treasury. The financial system is the underpinning of our economic strength. Why is there no equivalent of that inside of treasury? You have weird, interesting little pieces like

OFR, but they really are mostly in kind of exclusively pointed at more FSOC stability issues. So I hope that they would consider something like illicit, like scaled illicit finance and integrity of the system as a whole to be part of stability. But I mean, even the first economists that were in TFI came after the sanctions review at the beginning of the Biden administration, and they were inside of a OFAC, not inside of FinCEN or benefiting all of TFI. There's a, like you said, this need for a rethink, whether through FFRDC, through think tank, through public partnership, through government, wherever.

But to bring that really, really big think because measuring the benefit of a deterrent is really, really difficult and really complex. So I agree with you, I think that that's the kind of effort that would be good. It's a longer term Manhattan Project and then some of the near term things that we know that we can at least start getting actions in motion on certain R&D sandbox approaches, fixing the enforcement, dismantling work around data. I think that those are some of the near term actions that can create operational space for the longer term fixes.

Jo Ann Barefoot: That little sound clip of what you just said, Carole, is almost like a microcosm of the challenge because you just used a whole bunch of acronyms that I'm pretty sure half of our audience doesn't even know what they stand for.

Carole House: You're right, and I definitely said DOD, so sorry, Department of War, OFR is the Office of Financial Research. Sorry, that supports the Financial Stability Oversight Committee.

Jo Ann Barefoot: [inaudible 00:41:00], so that's part of the point that we're talking about here is we have all these groups that are very specialized in doing what they do, and we need to figure out how to put it together. I think it can be helpful, and I know it's helpful in these kinds of discussions to differentiate between the tech problem solving capability versus the human systems legal frameworks and so on. And I will say as a general proposition, we see every day at AIR that the tech problems are mostly solvable and the human ones are the hard ones. But let me ask you that. Do we have the technology to reliably keep data safe if we're going to share it more widely? Secure and protecting privacy, should people have confidence that if we share more across country borders, across public and private, as you were saying, Ari, that can we use encryption techniques or privacy enhancing technologies, zero-knowledge proofs, whatever they are? What are the ways to be sure that if we create this much more robust sharing, that it won't lead to massive exposure?

Ari Redbord: Yeah, I'll let Carole or Matt dive in here just really quickly. I think we do. I think we have people that are certainly building this today, and I think it's getting better and better. I think we should be sharing less and using technology in order, like you mentioned, zero-knowledge proofs, I think that's a great example of how we could arguably share less or just what is needed as opposed to creating these giant honey pots of information to be stolen as we have today. Carole, I have heard you speak on this for years. Yeah, go for it.

Carole House: Sure. And I'm so curious what Matt has to say since he's literally built a RegTech tool to help implement some of these things and help investigators. I know that I'll first highlight a controversial view that I have, because I know that there are, and this isn't disagreeing with Ari, it's disagreeing with certain arguments that have been made from parts of the crypto industry where they've stated that they should not have to do things like share information like originator and beneficiary information because, "Well, this other country doesn't have, how do I know if it's being protected or whatever? Or that it may create a honey pot and a target for information." My own view was and remains that, "So just to be clear, you feel that you guys should be trusted to custody digital financial assets, but not the information to help you understand whether or not that is a designated person or ISIS or North Korea. Just to be clear, that is your position that you should be trusted to custody the digital asset, but not the information that allows you to comply with really important rules."

So lots of people have very strong feelings and response to that, and I get it, but I also do agree that there's lots of information that is being shared all the time that does not need to, and where it requires that nuance of really thinking about what are the attributes that are necessary in order to conduct what specific use cases on detecting suspiciosity, on issuing due process, because those features look different. Like someone's physical address may not be an indicator of whether or not they are illicit. The attribute of whether or not that physical address matches some other supported or given identity document, that may be the attribute that you care of. Does X match X1? But then maybe that only needs to be discoverable when law enforcement says, "Great, warrant. I'm going to go arrest this person because I've determined that they're part of a money laundering network supporting a cartel or whatever."

And that's when they should be able to get access to the underlying attributes. But there's other attributes that are a part of really understanding the risk profile of who you're dealing with. So it demands that kind of nuance. And the tech, like you said, is there, it's really the discussions around the governance practices and architectures, and that's where when industry says things like, homomorphic encryption, multiparty computation, zero knowledge proofs, all these fun privacy enhancing technologies, I agree. We in fact, were telling industry in 2018 that the future of crypto was going to be privacy tech because people were not going to want to publish their information on public unobscured ledgers forever.

So we knew that, but industry hasn't yet. I've not seen industry or governments come with a framework of here's the entire ecosystem architecture that allows for appropriate discover ability for the complexities of what is knowing your customer and their risk profile through the life cycle of account management as well as supporting suspicious transaction monitoring and supporting due process. And then that just gets expanded into more complexities because of cross border issues. But there's some opportunities there to really carve into the

tech, I think is mostly there. I think the issue is governance and policy frameworks.

Jo Ann Barefoot: Before you speak to it, Matt, I just want to observe that if that's right, and I believe you, because I hear this from so many people like you who have looked at it deeply. If that's right, then one of the hurdles to overcome is that the decision makers don't believe it. I think there's just a lot of ignorance, frankly, and skepticism that these things are doable and wouldn't be just creating even bigger nightmares. But go ahead, Matt.

Carole House: Yeah, and industry hasn't coalesced around an answer too.

Jo Ann Barefoot: Yeah, exactly. Exactly.

Matt Van Buskir...: I think one piece of this that we always default to is acting like the status quo is private and safe. And anyone who's worked in the industry, one of the ways information sharing happens under 314B today is literally emailing a Word document with a bunch of PII and it to someone else, and then password protecting that Word document and then sending the password separately in a different email as if that makes it secure. But literally, financial institution procedural procedures sometimes are still doing that type of thing. I also remember a prior experience where got an unencrypted email from a not to be named law enforcement agency with about 400 social security numbers unencrypted just saying, "Do you have any of these? They're involved in a CSAM activity." And I'm like, "You have just put me in violation of my own information security policy here because now I have a PII in an unencrypted environment." So I think we need to acknowledge number one, that the status quo is incredibly not private.

And the second thing I think is we should be willing to also entertain the question of whether do we really care about low level criminal activity? They say this when you're designing a fraud program, the correct level of fraud is not zero, because if you have zero fraud, you're also going to be, the only way you can achieve that is by also probably kicking out a whole bunch of good customers who otherwise they end up tripping some flags. If the correct amount of crime is not zero either, the only way to do that is to have a dystopian kind of government Big Brother control of all aspects of society. But we need to find a way to invert what we have today, which is that the most sophisticated large scale criminal actors never get caught because they make it too difficult to detect them. And we only catch the low level people, obviously is gross generalization.

I saw in the news yesterday one of the Epstein fallout elements, a famous person in Europe was saying first had resigned from whatever roles that they were involved in and also six companies that they were involved in were going to be shut down. And this person was the only board member of all six companies, and all six of them did not have any kind of clear purpose for why they exist. So

we have, one of the breakthroughs in my mind happened when I was sort of in an operational role trying to figure out how to implement any money laundering controls was realizing we didn't even need to, it was important to look for known suspicious activity patterns, but it was even more powerful to invert it and say, "Let's just train behavioral models based off of what our normal customers look like and then anything that has a behavioral fingerprint of normal activity is fine." And then you devote your investigator effort to look at the anomalies, like people who are unusual in different ways.

If we think about it next generation anti-money laundering paradigm here where like throw KYC, transaction monitoring, and all the other stuff that we do out the window as it's done today and go back to first principles on it and say, "Maybe we don't need to have KYC activity." I mean, you can kind of do this in the money transmitter world a little bit, but you don't have KYC activity below a certain threshold. But then you worry about money mules and you worry about people creating multiple accounts. But do we have the technology now to create a biometric linked proof of personhood token that cannot be replicated where it's not your identity and your address and all these other things being attached to it, but you can prove it's just only me engaging in this financial network. And then you increase the threshold of KYC on me if I start exceeding thresholds of activity. But then also if we have every financial transaction activity, sorry, I can't speak this morning.

Financial transactions happening on chain, and you can start to see when all these low-level actors kind of connect up behind the scenes, maybe five or 10 hops down the road, we've got machine learning tools here that can start to tease out the behavioral network, put networks together. I mean, CRM has done a phenomenal job as a company of deploying these types of tools. So to your point, Jo Ann, I feel like if we toss everything out the window and come back like and say, "What do we really care about here?" We don't want the really big sophisticated actors to be able to run reins around us.

We want to be able to preserve privacy at the individual level, and we want to have the ability for government to go in and figure out what's happening in aggregate. I think the combination of the various types of blockchain technologies, tokenizing assets, tokenizing identities, all these types of things, we put them together, you can kind of start to see the outlines of the next generation anti-money laundering approach that could make the anarcho-crypto people who don't want any identity out there, at least a little bit more comfortable with things while still ensuring that the big bad actors are interdictable so the government and anti-money laundering people will be on board with that. And I'd love to see us really sort of, maybe it's a mandate for AIR here to come in and actually create a thousand page paper on what the next generation looks like here.

Jo Ann Barefoot: So I have one thing I wanted talk about. If you guys would entertain another conversation, let me tell you some of the things that I'm thinking about. One is

we haven't really talked about agentic AI. And Matt, what you just said really ties into that as well. How are we going to have proof of agency and know your agent?

Matt Van Buskir...: One quick thing to toss in there, everyone in Twitter is blowing up about OpenClaw and all this stuff right now. Can we imagine Clawbot enabled criminal activity here? So, sorry. Scary thought to drop in there. Please continue.

Jo Ann Barefoot: Exactly.

Carole House: You're right, Ari's already, his company's already highlighting where there's script enabled money laundering and stuff that's allowed there. So yeah, this isn't even the future. This is literally possible right now.

Ari Redbord: I feel like we've done some of this, but yes, I mean, it could be 30 minutes plus of conversation just around this.

Jo Ann Barefoot: Yeah, yeah, because I want to circle back on digital identity. I want to circle back on, actually, I have a really fundamental question. One of the earliest things you went to in this conversation was the need for asset recovery. I don't have a good sense of how well we know who's got the assets in this situation because you have to do that before you can get the assets back from them. I mean, are we mostly not knowing? Are we mostly in the dark on who's done these crimes or do we have a good handle on it often?

Ari Redbord: You mean when we're seizing assets?

Jo Ann Barefoot: I mean before we seize assets, how do we know who has-

Ari Redbord: That would be one thing that's kind of interesting. And Matt and I have maybe a nice cadence around this. I mean, we can describe a little bit more granularly what exactly we do in terms of attributing addresses, tracing funds and trying to do that work. How does law enforcement then or national security agencies make that association and kind of the seizure part and then maybe, Matt, into how that plays with how a compliance team using technology is playing a role in that process.

Jo Ann Barefoot: So are you all okay to do a follow-up? Matt, you look like you were going to say something.

Matt Van Buskir...: Yeah, if I could make a proposal, maybe this should be not necessarily a follow-up, but some combination of us could be, we should maybe make a goal of saying, "What do people really need to understand to make this change happen?" And do a series of episodes where we bring in some other people too.

Jo Ann Barefoot: I would love that.

Matt Van Buskir...: Like small panels. It could be really interesting.

Jo Ann Barefoot: Let's do it. Okay. We need to let you go, Ari, in one minute and I'm going, or maybe you're going to tell me you can't do it, but do you have a last word for us before you drop off?

Ari Redbord: Oh, sure. Do I have a last word for you? Gosh, I feel like we've had so many last words. Great last words today. Look, the way I think about this space, and honestly the way I think about life and the way I work and the way we operate is speed. I joke that I love to run and move fast and all of this. I think right now we're living in an era of just unprecedented speed and bad actors are leveraging the ability to move faster than ever before. And AI is supercharging that activity. And to me, the challenge is building policies, procedures, programs, technology that allow us to move faster than those bad actors. I love that Matt loves the story of the Ford Model T rolling off the assembly line and having to stand up the FBI, but it really is true. We need to ensure that we're using the same technology to move fast, to move cross border as the bad actors are. Whether that was automobiles, end-to-end encrypted messaging apps, the internet, crypto, and now AI.

Jo Ann Barefoot: Perfect. That's where you started, Carole. That we can't keep up, we're not keeping up and we have to solve that. And it's not going to be easy, but it has to be done. There's not a choice, really. So we're going to let you go, Ari, and then I'm going to-

Ari Redbord: Thank you so much, guys. Really appreciate it.

Jo Ann Barefoot: Thank you for joining us.

Ari Redbord: Awesome. Great to see you. So much fun.

Jo Ann Barefoot: Amazing.

Ari Redbord: Bye, guys.

Jo Ann Barefoot: Bye.

Carole House: Bye.

Jo Ann Barefoot: Carole, last word from you for today?

Carole House: Yeah, we need to focus on the things that we can make meaningful progress on in the near term to create the operational space for those longer term efforts. So in the near term, it means certainly stopping the dismantling of enforcement and analytic and regulatory work and controls. But instead resourcing them with money, people, and tools and then giving them the mandate to go to prioritize the most egregious violators and not just those that are the easiest to get our

hands on, which are often US operating firms. That will help to balance the concerns that have come from industry on arbitrary enforcement and demands that government agencies think very hard about what is the data and analytic that they need in order to assess who are in fact the most egregious violators in the space. And that really frustrated me after the FinCEN files leak, which was heinous.

But when people were saying, "Oh, well, this is evidence of how illicit and corrupt all these institutions are." And I'm not saying that anyone's perfect, but these are the ones that are filing. I'm just saying that this is a misunderstanding of what's going on. So thinking about that on the enforcement side, working on that on the data side, and then leveraging through carrots and sticks, political will for actually actioning with financial institutions in the tech sector to do something about it. In the medium term, figuring out the sandbox and digital identity and AI architecture re-envisionings and frameworks and what does efficacy truly look like. And then in the longterm, fixing the underlying issues around dollar dominance. China just released a strategy that is terrifying and that we are not meaningfully addressing. And when coupled with things like that, my own personal view, is that a US entity to win the fight on US dollar denominated stablecoins, not to mention more broadly innovations and digital payments.

So lots of things there. And then broader, tougher issues on things like liability and accountability in software and decentralization and digital economies. Those issues keep coming up and rearing their heads and people keep trying to address those now. Those are the sticky, really, really tough issues. Those need to be thought of in a more holistic, strategic way. So that's the longer term stuff that needs to be thought of as part of an entire architecture of digital economy accountability. But we need to bucket it as thinking about what the near-term things are on identity fixes, enforcement fixes, data fixes and public-private partnerships, medium-term, broader efficacy and re-envisioning innovation frameworks and integration, and then longer-term problems on dominance and accountability in the digital domain.

Jo Ann Barefoot: Thank you. Matt, you got the last word.

Matt Van Buskir...: No pressure. I think combining the themes of what Carole and Aria were just saying, our entire regulatory system has been designed to be methodical and deliberative, and that means slow. And to Ari's point, the criminal world moves incredibly fast. But to Carole's point also, we haven't really faced geopolitical competition in my lifetime really. We now do have credible competition from China that we need to be reactive to. And I feel like I've seen a lot of, we have a lot of approaches, the default thinking regulations is sort of like, America is always going to be the dominant financial player in the world, therefore, we can take our time and do what we want and the rest of the world will follow. That's not true anymore. We may make decisions that will cause a large portion of the world to move out of our sphere of influence and into China's.

So our regulators need to actually be accounting for whether our economy and our country as a whole is going to be competitive and innovative in a geopolitical sense. And then whether or not we're sitting ducks from the criminal sense as well. And this is why this is like, I think Carole's completely right, that we need to be doing things tactically to be buying ourselves the bandwidth needed to do more. But I think we really need to be finding ways to get a lot of funding behind the geopolitical, high level strategic type thinking as well. Because I mean, being in the government, we all know, we've all been there. The way you operate is fairly confined. There's a lot of micromanagement going on, there's not a lot of bandwidth for people to really take a step back and do this high-level thinking.

We need to find ways to make it easy for them. And back to Ari's point, this is true public-private partnership. The private sector should be thinking about this stuff as if they were the government and not just advocating for their own little niche of business to lobby for some advantage there. But we need to be thinking about America as a whole being more competitive or the West as a whole being more competitive. And I really hope that we start to see, I think that a lot of us in our community are fired up to try to figure out how to do this, but we don't really know. There's a lot of spinning of wheels because we don't really know what direction to all go into. So I hope we can kind of crystallize efforts to actually put everyone's minds together and come up with a comprehensive plan.

Jo Ann Barefoot: So let's think about in future shows, and as you said, Matt, in some of the work of AIR, can we begin to identify those practical steps that need to happen to be finding the pathway? And quickly, back to Ari's point on this, because there's so many, the technology is making solutions possible. Technology is making the problem worse and it has to have technology driven solutions. And those solutions are making it possible to do things we couldn't have done even recently if we can get ourselves together to put them to good use. So, all right, I cannot tell you how much I appreciate both of you and Ari, and we'll be circling back with some more great conversation on this one way or the other. So thank you both and we'll put in the show notes how people can find you and tap into the amazing work that you're all doing. So thank you both. Bye.

Matt Van Buskir...: Thank you.

Carole House: Bye.