Barefoot Innovation Podcast: Carole House, CEO of Penumbra Strategies, Ari Redbord, Global Head of Policy, TRM Labs, and Matt Van Buskirk, Co-Founder of Hummingbird

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

Jo Ann Barefoot:	00:03	I have been looking forward to today's show for a long time because we are going to have an amazing conversation with three of the smartest, bravest, most interesting people I know in the field of combating financial crime, and I think you're really, really going to enjoy it. I'm going to ask my guests to introduce themselves and why don't we do it in order. They're Carole House, Ari Redbord, and Matt Van Buskirk. Carole, let's start with you. Just tell people a little bit about you and don't be modest.
Carole House:	00:42	Well, I'll start off by first saying that I'm a giant fangirl of everybody else on this podcast, but I am Carole House. I'm currently CEO of Penumbra Strategies, a strategic technology and national security advisory firm, and just doing a lot of advisory and board work for founders and for big companies trying to figure out how to get the nexus of national security in tech right. But I've spent my whole career at this intersection of national security and technology and being wherever bad guys are, trying to use tech to hurt Americans, I want to try to be there to stop them. Started Army, chem, bio, rad, nuclear and intelligence work. And then I've done time at the Senate Committee on Homeland Security as well as at Treasury, the Financial Crimes Enforcement Network, where I led crypto, cyber and identity policy for a little under five years.
	01:31	And I've done three tours in the White House, including twice at the National Security Council, like driving work on digital assets on other illicit finance and things like ransomware where you get the cross-section between things like cybersecurity and cryptocurrency. So it's been a great place to work where I've had the privilege of working with again everybody on this call. So the most important part is really that I'm a huge fangirl of everybody here.
Jo Ann Barefoot:	01:56	Wonderful. Ari, how about you?
Ari Redbord:	01:59	What a love fest. I feel the same way. It's really an extraordinary opportunity to be really talking to friends today. And I feel like with Matt and Carole, I've had so many private conversations over the years about a lot of the issues we'll talk about, and it'll

be fun to be able to talk about them then publicly. I'm Ari Redbord, the global head of policy at TRM Labs. We're a blockchain intelligence company and we can sort of get deeper in that, but it means we work with law enforcement regulators and compliance teams globally to mitigate illicit finance risk in cryptocurrencies. Prior to joining TRM about five years ago, I spent about 11 years at the US department of Justice. I was an AUSA for the District of Columbia, really working at that intersection of national security and money laundering, what I call threat finances, stopping bad actors from getting the funds they need to do bad things, terrorist financiers, sanctions, export control.

02:51 I then spent about two years working with Carole closely at the US treasury Department where I was the senior adviser to the undersecretary and the deputy secretary working on illicit finance issues, sort of overseeing the national security apparatus, FinCEN, where Carole worked, OFAC, et cetera. So thank you, Jo Ann. You are a legend in this space and really excited for the conversation today.

Jo Ann Barefoot: 03:15 Thank you. Thank you. And Matt.

Matt Van Buskir...: 03:19 I would say in contrast, the illustrious government careers of everyone else in the group here, I was also the government, but I started my career as a junior bank examiner during the financial crisis, which was quite a learning environment, but promptly left the government when the OCC merger happened, and most of my career has been outside of it. So I'm a co-founder of a company called Hummingbird. We are a partner of companies like TRM, and we work pretty closely with Ari on that, enabling global case management.

03:50 We have a belief that the future of the fight against Fin crime is going to rely on modular technology solutions that will be cutting across both public and private sector data sources. And prior to launching Hummingbird, I met my co-founder at Circle where I was the first head of compliance, built out the compliance stack there. My co-founder was in charge of building out the risk stack. So that's where we start collaborating pretty closely and ended up leading to the creation of Hummingbird. So I'm very excited for this conversation. Also, I feel like this is one of the podcast episodes where everyone is actually in DC within a fairly close distance of each other. So it's kind of a fun thing.

Jo Ann Barefoot:	04:27	Probably should have sat together over a glass of beer or something. But here we are. And full disclosure, I too was a co-founder of Hummingbird, I think, was it eight years ago, Matt now or seven?
Matt Van Buskir...:	04:41	Coming up on 10.
Jo Ann Barefoot:	04:41	Oh my God.
Matt Van Buskir...:	04:41	Next year.
Jo Ann Barefoot:	04:44	So I'm not actively involved with Hummingbird and have not been since the very early days, but I've been fascinated to see the progress. So I have said to you all, everybody knows that financial crime is a big problem. Everyone knows that it's increasing. But one of my goals for today's show is I think I said to you all to try to scare everybody to death, to take this as seriously as it needs to be taken. The delta between the curve of rising crime and the severity and novelty of these crimes versus the progress that we're making in solving them is growing by the day. The forces of the good guys are falling behind the bad guys, in my opinion. Again, well, if people don't agree, speak up. And so I want to start by just talking about what's happening out there, and Carole, let's start with you. What's the magnitude of this problem? What are the particularly troubling trends that you're seeing and so on?
Carole House:	05:59	Yeah, well, it's funny since one of the ways, the most impactful way that I've heard it described at times on what the illicit finance economy looks like was actually from you, Jo Ann and Matt earlier this year at a retreat that you hosted where you just highlighted that the threat finance economy is a G7 economy. And that's totally right. We've seen estimates that have come out, even NASDAQ just published their global financial crime report where they highlighted that just in 2023, it was $3 trillion that was moving through the financial system of illicit funds just on fraud alone. You've seen estimates that range somewhere between 500 billion up to a trillion dollars. And I'll tell you, I think it's more than that. I think it's way more than just 1 trillion. The US government alone had an estimate last year highlighting that the US government loses somewhere between around 250 and $512 billion a year to fraud.
	06:58	So that's not just the direct fraud losses, that's also the broader impact of remediation and broader impacts that you get on lines of business, et cetera. But that highlights that the economic impact that's happening to nations and to this economy is

absolutely massive and pervasive. But then also the devastation that is being wrought on consumers more broadly. We saw AI-enabled scams, we estimate saying that AI-enabled fraud has skyrocketed around 500% just over the last year or two. And we're seeing state actors that are leveraging emerging technologies to support their ability to conduct more sophisticated spear phishing campaigns to target people in really sophisticated ways. Seeing illicit to state actors targeting sectors, including the cryptocurrency sector that we all work in to try to defraud people. And most phishing emails that are sent now are honed because of the democratized access to these amazing capabilities that are offering so much great capacity for good, but also have provided democratized access to a lot of illicit actors that's happening.

08:06 And so we're seeing just billions of dollars being lost and harvested from consumers, not to mention the human impact that's happening, where now the person scamming you has in fact been scammed and is sitting having been trafficked in these cyber scam compounds. And it's just, it's a complete confluence and convergence of these emerging technologies when we haven't built in the trust tech underlying rails to make it really a fair fight or to scale the good guy's ability to detect and combat this. And then we're seeing enforcement activities that inciting actions from years ago. So we're not seeing enforcement actions getting more scaled and more timely, other than a couple of instances where there have been some good cases of us taking down major compounds like for example in these fraud networks. They're still citing activity from years ago. The impact is still very real and happening and tangible, and those aren't the only actors that are out there.

09:12 So you mentioned wanting to scare people. I'm really worried that we've not invested in those underlying trust tech infrastructure and rails that's needed. And now with the aggregation of a lot of different emerging technologies that each have their own challenges with responsibility and accountability, I think that we've got a few years ahead of us of some really tough time in trying to combat and wrap our arms around this problem, especially as we're firing thousands of regulators. So other metrics that are really worrying where we're taking out a lot of different pieces that are necessary for a really effective AML framework.

Jo Ann Barefoot: 09:48 And I should say for the purpose of this conversation, and actually for the purpose of a lot of the work that AIR does in this space, we are defining illicit finance for financial crime broadly.

It actually in the real world tends to live in silos where we have an anti-money laundering community and an anti-fraud and scam community and cyber is its own field and so on. But these crimes have a lot in common in terms of what causes them and we think what can combat them. So I want you all to speak to any aspect of this that is resonating with you. Ari and Matt, do you want to add anything to the scope?

Ari Redbord: 10:34 Yeah, Carole took you very seriously when you asked her to scare people. And I'm famously optimistic in terms of sort of the tools that are being built out there and the way they're being provided to law enforcement to investigate and ultimately mitigate a lot of what Carole spoke about. But she absolutely nailed the issues. I think she actually either intentionally or inadvertently cited, I think a TRM number that we've seen about 500% of increase in AI-enabled scams over the last year, which is pretty extraordinary. And to Carole's point, without repeating too much of it, this allows bad actors to basically perfect the activities that they've done for so many years, right? I don't know that AI has changed illicit finance or scam activity, but it is supercharged it. So now the phishing emails that used to have broken English are now perfected for the listener on the other end.

11:29 And we're seeing deepfake videos used at scale now and phone calls using voice of loved ones in order to convey importance and urgency. So I think what we're seeing is technology really utilized by bad actors at scale. Matt and I, hosted an event in Vegas a few months ago at the Mob Museum, and I told the story of how in 1908 as Model T's rolled off the assembly line, America created the FBI essentially because we were seeing all of a sudden bad actors be able to move across state lines, unprecedented speed and scale. And we needed a national police force in order to track and trace and follow them across state lines.

12:18 Bad actors have always been early adopters of transformative technology, and that's true with AI, that's true with crypto, that's true with end-to-end encrypted messaging applications. So the reality is we now need the good guys to make sure that they are also leveraging these tools, and we're building AI solutions at every layer of our platform at TRM today to try to keep up with bad actors. It's this constant cat and mouse game that you've dealt with your entire career, Jo Ann and Matt, and compliance. This is always the game. It's how do we move faster as bad actors are moving faster? And we can dig into a lot of that today.

Jo Ann Barefoot:	12:54	Yeah, we're going to turn to the solutions in a moment, but Matt, what would you like to add in terms of understanding the magnitude of the challenge?
Matt Van Buskir...:	13:03	Ari really one up to me in the intro speech at the Mob Museum there having an excellent story to tell where I was just prepared to say, "Thank you all for coming." It's a little, I should have done some research in events. We co-hosted an event last week in London on wildlife trafficking, and I was introduced to a term I had never heard before, which is poly-criminality. And I'm not sure how widely used it is, but at least they said it's going around the UK. And the way they describe it basically is saying if you're a bad guy doing one thing, you're likely to be interested in doing other bad things. And as these criminal organizations that have made a lot of money through narcotics or weapons trafficking or whatever it would be, they are branching out and doing things like committing fraud and scams and they're specialized in, it's becoming a very organized business.
	13:59	I think everyone here has listened to the Economist series called Scams Inc. And the reason they called it Scams Inc is making the point that this is a multinational business. People feel like they're being tricked by some scammer on the other side of the world who is personally taking advantage of them. And to Carole's point, no, they're just a cog in the machine and often are victims themselves. I think leading into the next steps, Ari, you mentioned this as a compliance piece. I feel like one of the biggest problems we have had traditionally in our fight against the bad guys here, at least on the financial industry side of things, is we've been treating it like a compliance problem. And for most of other areas of compliance, we don't have adversaries. It's people making mistakes, people skirting around systems and financial institutions, but we don't actually have an intelligent bad guy who is trying to subvert everything we're doing.
	14:53	And I don't think we can continue to treat financial crime like a compliance exercise in financial industry. We can't have regulators who are disconnected from law enforcement and understand exactly what law enforcement needs in order to achieve the goal of interdicting flows of funds and actually arresting the bad guys. The other kind of scary point I heard in the last week was saying that the economies of scale that will be delivered by all of the criminal organizations adopting AI means that historically they've been going after fairly wealthy people, retirees and such who may have enough money that they can go drain their retirement accounts through romance scams. But

with the explosion in AI capabilities and maybe become economically viable to go after someone where their life savings is $50 if it's a fully automated and executed scam operation. So this is not, right now, this is a wealthy world problem, but I think it's increasingly going to become a global problem where it doesn't matter who you are or where you are, you could be a target and we need to stop treating this like it's not an existential fight.

Jo Ann Barefoot: 16:05 Yeah, those are great points. I was at a international roundtable yesterday on fraud and scams as they're affecting the silver economy and meaning older consumers. And one of the people made the point that in parts of the world, people are getting old before they are getting rich and they are targets for this, and then they are being completely wiped out by it.

16:41 There were people who cited statistics, one was for the US and the other was a global survey, both of which found that about one in five people have been directly victimized by a scam. And if you count how many of us have had loved ones and people close to us. When I speak to audiences, I often ask that as a question. And if you ask how many people here have either been subject to a scam or fraud attempt or have a loved one or someone close to you who has, almost every hand goes up. I mean, it's just becoming ubiquitous. And Matt, I think it was you who said to me a while ago that these crimes are now bigger than the international drug trade. It's more lucrative and just bigger business. So you can't solve that with little piecemeal compliance steps. You really have to marshal your energy.

17:42 And just before we move on to the solutions, just to reinforce the human side of the problem, as you said, Matt, a lot of the people who are involved in these crimes are victims themselves. They are in modern human slavery and captivity. They're working in call center somewhere where they've been a call center or a tech center of some kind where they're perpetuating these scams. And then we increasingly are seeing the rising profits from these crimes being laundered through the money laundering apparatus. So again, merging between these types of crimes that have tended to have sort of siloed treatment. And a huge amount of it is being laundered because it's so profitable to do human trafficking or drug trafficking or wildlife trafficking and so on and ruining people's lives completely. And we also know that scams are underreported because many people are embarrassed and feel ashamed that they fell for it and don't want to talk about it.

Ari Redbord:	19:00	Jo Ann, one thing that you and Matt both mentioned in this, and just a super quick comment maybe to put a point on it, is you mentioned how a lot of times we're approaching these different categories or different issues as siloed. We have always dealt with scam and fraud activity as a law enforcement imperative, to go after bad actors that way. North Korea is a place where we have used sort of national security tools. Carole was very out front of that in that when she was at the White House, cartels is something that drug trade has always been typically sort of a law enforcement. I think this administration has moved it more into the national security realm. But what we're seeing on blockchains at TRM is we're seeing indicia that all three of these typologies are connected through Chinese money laundering organizations. The same organizations. In fact, some of the same wallet addresses that we see involved in, say a North Korea hack, the Bybit hat for example, is connected to funds moving through cartel activity and is connected to funds moving through these pig butchering networks.
	20:02	So just kind of put a on-chain point on what I think has been said, we're seeing a real convergence of this type of activity, which to me makes it an absolute national security imperative. And I was really thrilled last week to see us use sanctions and criminal indictments and civil forfeiture and travel bans and all the things we used and the UK used with the United States in the Prince case to try to take down that scam network.
Jo Ann Barefoot:	20:34	Yeah, that's so well taken. So go ahead, Carole.
Carole House:	20:39	Yeah, since you had mentioned that people are embarrassed to highlight it, I just learned a week and a half ago that an immediate family member was scammed a few weeks ago and they were too embarrassed to tell me because it's something that I'm constantly talking about everywhere, including with my family. And it was so horrible to hear about it and the way that they went after them, they went after them based on their veteran status and specifically targeting this community because they're known for being helpful to other veterans in need. And that was a part of the scam that was leveraged, and it was just horrific to hear, and it was crushing. It always is with victims. But then to even know that my own family member didn't tell me until just about a week and a half ago, and I love... The point that you've mentioned to the silos, Ari, also highlighting this issue of the fact that these are arbitrary, these are arbitrary walls that everyone on this call has been trying to fight for years.

	21:46	And it's such a problem because those are exactly the seams that these organized crime groups are counting on and leveraging and exploiting because they're believing that the inefficiencies of governments, and that's just internally across different agencies and of due process processes mixed with the regulatory processes and capabilities and then the barriers to industry. And then inside of industry, all the fraud and cyber and AML functioning separately, and that looks different across each institution, all of that. We have North Korea weaponizing cyber-enabled fraud networks to circumvent sanctions and got the multilateral sanctions monitoring team just came out publishing a study. So this is the group that basically advises the UN monitors for how compliance is going with National Security Council resolutions, sorry, UN Security Council resolutions, excuse me. And they highlighted the $3 billion that North Korea has been leveraging and stealing through cybercrime, crypto heists and DPRK IT workers over the last year and a half or so.
	22:48	But all of this global syndicates, operating romance and investment scams, leveraging these enclaves and Myanmar and Cambodia, partnering with militias and corrupt elites to funnel these proceeds. It's this weird blend of the asymmetric advantages and asymmetric warfare and leveraging tech to scale that capability and the challenges that we've had with that. And then kind of economic warfare. It's these horrible corollaries that have just made us, we are not scaled. And I know Jo Ann, you're leading us into this discussion of what the heck do we do about this? And you're always pushing the needle on how do we solve this, but these are really tough issues that we have problems with individually, and now they're each reinforcing each other in some of the toughest ways that the government has a really, really tough time scaling to address.
Jo Ann Barefoot:	23:40	Yeah, we did a recent show with Dave Dewhurst at DARPA, and I'll link to it in the show notes. And at DARPA has, as this group knows, elevated this topic to be a national security priority and are working on tech solutions for it. And one of the things that Dave said was that more than half of the North Korean nuclear missile program is paid for by scam money from the west. So huge, huge, huge problem. And it's getting worse instead of better. So our listeners have heard me say, if we've done 250 shows, I've probably said 100 times at least, that the system we have now is not working. The problem is getting, or it hasn't been working. And we're going to talk a little bit about the cost benefit balance here. But it's, for the banking industry, massive resources go into compliance. It's the most expensive compliance thing that banks do.

	24:53	And at the same time, the famous UN number, which is dated now, but it's probably worse than it was then, is that with all that effort by both public and private sectors, we're catching at best maybe 1% of the crimes. And so we have a model today that isn't working and we're losing ground, partly because the technology is driving the criminals. As one of you said a minute ago, you've got the arms race going on where you just constantly are trying to catch up with what they're doing, the creativity and the tools that they're using. So let me ask you broadly, what is the most important thing that we need to change?
Matt Van Buskir...:	25:50	I'll jump in, and one thing that struck me from my time at Circle, starting to interact more closely with the law enforcement community, was learning from a policing side of things. How we think about these crimes as in the money laundering world where you have the concept of predicate crimes, which is whatever crime was committed to then produce the money that then needed to be laundered. But when we tend to think about combating crime, it's like the war against drugs. It's the war against poaching or whatever it would be. I learned last week also that the glass eel poaching industry is a $3 billion industry, and I didn't even know what a glass eel was before last week.
Jo Ann Barefoot:	26:41	What is it?
Matt Van Buskir...:	26:41	They're juvenile eels.
Jo Ann Barefoot:	26:42	Eels.
Matt Van Buskir...:	26:45	Yeah. Without getting fully in the weeds, they basically become seed stock for people who are then going to be raising them as a food, a cultivated food source. So they get them illegally, but then it can become a legal business down the road. You don't really know where the eels came from. So we think about-
Jo Ann Barefoot:	26:45	That's a $3 billion industry did you say?
Matt Van Buskir...:	26:45	Yeah.
Jo Ann Barefoot:	26:45	Wow.
Matt Van Buskir...:	27:08	So think about glass eels, $3 billion. Think about all these different little things all over the place that are multibillion-dollar a year industries. And the people going after the glass eel industry are basically anti-poaching type experts or anti-illegal fishing type experts. The thing that, they are all

committing these crimes in order to make money and the way that we need to treat all this stuff is saying still go after policing the front end of it.

27:38 Another thing they were saying on the poaching side of things, the people doing the poaching are making almost no money. They're typically fairly really economically disadvantaged people. Arresting them doesn't stop them. Other people from the local area will probably try fill that gap. And there's almost no enforcement once the product has been delivered into its destination, they started experimenting with legal sales of ivory apparently as a means of trying to undo some of the demand. And they said it was a massively failed experiment in their early 2000s, where, by making it legal for a little while, they massively increased demand. And then over the subsequent seven years, something like a third of all the elephants in Africa were killed.

28:26 So we need to be viewing this as having adversaries where they have a business model that they're pursuing, and we need to be finding ways to interrupt their business model where at stages where it hurts them the most economically, not where they can just replace a little cog in the wheel like an individual money mule or an individual scammer. Those don't matter. We need to find the ways to go and do the $15 billion seizures and all those types of things and make it really hurt them economically and maybe change the economics of how they actually perpetrate these crimes. So I know, I'm going to see Carole and Ari both nodding probably. This is something I may get a little too fired up about, so I'll pause for now.

Ari Redbord: 29:08 No, we all get fired up. We all get fired up about. I'll let Carole go, because I think she's particularly fired up and I'll jump in after you.

Carole House: 29:18 Oh yeah, I love this. And the way that you framed it of like, "What is wrong? What is happening?" And I totally agree, Matt, this issue of the way that we're enforcing it's not working. And some of this starts from the very beginning of the problem that, I'm going to start with the problem that AML as a framework has on its defense because I am defensive of it coming from FinCEN, so take what I say with a grain of salt, but given that we're all counter-financial crime professionals, I suspect that we'll agree on this, but AML is a really tough framework to defend. In the cyber security world and a lot of the operational risk and credit and counterparty and market risk, you can defend that most of those practices that need to get put in place. I understand that there's still some fights around whether

the controls are the right ones, but generally those frameworks, those controls will help keep you alive as a business.

30:06 If you suck at cyber, you will go under because your intellectual property will be stolen, your money will be stolen. Money laundering is great business. It's a horrible way to say that, but it just is. Money laundering is great business. The effects of money laundering and the things that are attached to them are not great business. And that was the whole point of why the Patriot Act helped to expand these authorities capabilities is because 9/11 isn't good for business. Human trafficking isn't good for business and cybercrime and fraud and all these other things are not good for business, but it feels less connected, it's less direct, so you can't defend it as easily. And this is the framework that people view as this is the thing that infringes upon your privacy. And especially in a world where we have enabled the rise of with data aggregation services and others where data harvesting is what so many businesses are based on today, people are very concerned.

31:06 In fact, it's where both sides of the aisle really end up meeting each other, in fact on being concerns about privacy issue. So that puts AML in a really tough place to defend. And I know that you're going to drive us through a really needed discussion on efficacy and the issues with AML, but that's one of the toughest issues is just that the framework is tough to defend and we need to get into how we need to make it stronger to defend. But then our core processes have not scaled to try to address the issues on prevention, detection, disruption and redress. I feel like this is the way that I see that the fixes that you need at each stage in the process are different. And even if we've gotten better at one thing, we've not gotten better at another. On the disruption side, we just settled the case with ShapeShift was an example of a mixer that had facilitated illicit activity. We just settled that case a couple of weeks ago.

32:02 It stopped existing in 2021, this mixer, and it was citing activity from 2011. This is the timeliness that we have for our, and I know that there are other enforcement actions that are more timely. So this was a bit of a reach on highlighting some of those timeline issues. But this problem of the due process takes a long time. Many of our enforcement cases are taking many, many years after the fact, which isn't doing anything for the harm that's being wrought in the middle. And while there are efforts like Operation Level Up and other things on ransomware where the FBI was doing victim notification to help decrypt systems while they were doing the Hive takedown.

	32:41	There's things that are happening, but it's not a comprehensive scaling of our capacity on the defensive side and prevention through things like investment in digital identity. On the better detection side, so enabling data taxonomies and schemas and better use of AI and cross-industry information sharing, scaling enforcement, the tools and capability, and then of course investing in redress. It's just not happening. And I think that tees up well to Airy given that their tool that's trying to scale and use some emerging technologies to address some of this problem.
Ari Redbord:	33:15	No, I always appreciate a good segue. Thank you. Thank you, Carole. Look, I think that predictably, I would say certainly sort of tracing and tracking cryptocurrency is an important piece of this, but tracking and tracing funds on blockchains is not going to solve this. And I think to what, Carole, to all the points that Carole made, we need to really turn this into a national security imperative and not just talk about illicit finance as a big problem, but talk about the component parts to some extent. We should be going, when North Korea steals 1.5 billion from a cryptocurrency exchange, we should be stealing it back.
	33:50	There's no world we shouldn't be attacking our adversaries the same way they are attacking lawful businesses using offensive cyber and other means other national security tools. Maybe controversially, maybe not. I think the war on cartels that this administration is executing is exactly the type of activity we should be doing. I think we should be treating these organizations as the terrorists that they are, using every type of DOD and national security authority against them. I think the Prince example from last week is a great example of how we can combine law enforcement and national security authorities to go after these pig butchering networks.
	34:32	I mentioned earlier that sort of all roads lead to China when it comes to the laundering of these funds. So what do we do about that? When I was a prosecutor, I was with a small group of folks from DOJ and the FBI and elsewhere, I worked with a wonderful colleague, Zia Faruqui, who's now a federal judge in DC. And we were still the first and still to this day, only prosecutors to ever serve a Patriot Act subpoena on a Chinese bank that was involved in North Korea money laundering. We should do that. And if they don't comply, we should cut them off from US correspondent banking and send a message there. We should be using the State Department in every diplomatic lever that we possibly have to go after China and ensure that they're taking this type of activity seriously. So I'll get off my soapbox

because this is definitely my soapbox, but I do think it's every tool and it's really, really putting the pressure on China.

Matt Van Buskir...: 35:24 The DARPA briefing, when they were kicking off the A3ML program, I was obviously only able to attend the unclassified portion. They kicked me and everyone else out of the room who did not have a clearance for the second half. But one of the unclassified data points they gave other than the North Korea data point we've already had is saying that the intelligence community estimate is $2 trillion annually of financial crime has an access to China. And this grew out of a lot of basically laundering as a service being offered to the Mexican and South American cartels and that they became so good at it that it became a service they started offering elsewhere. And this is where once again, it's becoming, it is a business model that they're pursuing.

36:09 Yeah, the downstream effects of this stuff and treating, money laundering is not a white collar crime. It's enabling all of this other stuff. It's enabling terrorist attacks all over the world, assassinations, all sorts of things. So it is, for not having a military background. I may get the analogy wrong here, but it's like a combined arms type of response is what we, I think need to come up with here.

Jo Ann Barefoot: 36:37 So I'm actually going to exercise the prerogative of the podcast host and say that I would like to make this part one of a two-part show because I know we've got 15 or 20 minutes left today and we are opening up so many topics. If you're all willing to come back again, we'll enable ourselves to go further with it.

Ari Redbord: 37:03 Didn't you just promise earlier in person and over beers or something? I thought you said that to kick things off.

Carole House: 37:03 I love it.

Jo Ann Barefoot: 37:11 I would definitely [inaudible 00:37:13]. So back to this question of how to scale. We know that the criminals and terrorists are using all the tools and especially now the generative AI tools, massively scaling up their attacks. There's no possible way that the consumer, even though it's important to educate people and all that, we're not going to be able to educate people into defending against every sophisticated attack that comes up at them. How are we going to scale up the defenses or the counter-attacking, as you say, Ari, and where is the role of technology and better data? You said, Ari, that we're not going

to solve this with blockchain data analysis, but we need blockchain data analysis.

Ari Redbord:	38:10	Sure. It's definitely a combination of things. And I think, look, the thing that AI was literally built for is just this activity. It's taking all these extraordinary data sites sets that we have across the public sector, and that obviously includes on-chain activity like the databases we have at TRM, but it's much more beyond that, right? It's shipping records and beneficial ownership and sort of all this data that we have. And really to put AI on top of that and to really help law enforcement and regulators have real-time insights.
	38:41	Let me give you a really fun example. About a month or so ago, late August, we announced at TRM this thing called the Beacon Network, which is a public-private partnership where we brought together the entire crypto industry. We believe it's about 80% of all centralized transaction volume in crypto is represented within Beacon. So think Coinbase, Binance, OKX, Kraken, crypto.com, blockchain.com, also fintechs like Robinhood and Stripe and PayPal. And we have combined that with the power of global law enforcement, so US, UK, APAC, and basically trying to create a perimeter around the crypto ecosystem to stop bad guys from being able to off-ramp funds.
	39:23	And I say that, and you mentioned data, data is obviously a huge piece of this, but it's, Hey, can we really, really leverage the expertise of the private sector with all of the authorities that the public sector has to get very, very serious. Just public-private partnerships, in my mind, and I know this is sometimes controversial, should not be sitting around the table sharing best practices. They should be real-time interdiction and seizure of illicit proceeds. And that's the kind of stuff that we need to build together. Private sector does that really well. Hummingbird is a great example here. You can provide the tools to the private sector and it's like how closely can you work with law enforcement in order to take the tooling that you have and then really go after the funds that only law enforcement can do at the end of the day?
Matt Van Buskir...:	40:10	I have a data anecdote here. I have a friend who fell for a scam and the situation was a relative passed away and there was an estate sale going on and he got targeted through Facebook and bought a truck from the relative who died. It didn't realize that it was actually a scammer who had mined all of the data in their friend network to understand when the funeral was happening, what the estate sale was going on with, and basically just

mirrored it, created a fake pitch. And he didn't know that. Yeah, he didn't know that it wasn't real until he went to pick up the truck. So that's the level of sophistication we're dealing with here. There's incredible data mining coming across all different silos in order to create this type of targeting.

41:02 We need to have a, I think Ari, you make a really key point here. AI is made for this on the good guy side of things as well. You can't expect a human analyst to be plugging into 80 different data consortia to put the signals together and figure out what's going on. But AI could do that. And this is where I feel like maybe episode two here, for those of us in the world that care about freedom and privacy and all of that, you could have a sort of dystopian and big brother path here where you create a social credit score equivalent type of thing where everything about all of our activities being tracked. And yes, we would cut out all the fraud and financial crime that way, but then those tools are very ripe for abuse.

41:49 I think that we need to be thinking about a techno democratic way to build this ecosystem out so that the data pipes exist, the tools exist, but we have created capabilities that have transparency and accountability such that we know that it's difficult for them to be abused. One data point I, come to think about it, some of the government databases we're all familiar with and some of the agencies on the back end there are running in such old versions of things like COBOL that they don't even have audit trail access. You can't really tell who initiated what query and when, and you're basically trusting... This came up with the, I don't remember who it was, but the data leaker ended up being indicted.

42:42 I apologize, I'm blanking on it, but it was, you guys will know I'm talking about. When they're tracing it back, I saw a senator commented after that saying, "When we have everything classified as top secret and then therefore have to give 3 million people top secret clearances, is anything actually secure at that point here?" So we've been relying on people as the control, like train them to do the right thing and then trust that they will not be compromised or won't make a mistake. Where we could actually build systems with the controls and protections in place today such that the system itself will force compliance, will still achieving what's needed. And that I think is the complex challenge we face here today because we're talking about all these different silos and their downstream effect of all the different laws that we've put into place here. A lot of this really is going to come back, I think to Congress and other legislative

bodies around the world redesigning how this all works and giving a mandate to the administrative branch people to do that.

Jo Ann Barefoot: 43:50 But what is the key to this? In many ways, this is a, other than the scale of the problem being so hard to attack, I think the other, to me thorniest problem is do we have to choose between privacy and anti-crime or can we have both? And can technology enable us to find a sweet spot where we're able to accomplish both goals? Carole, you look like you got a thought.

Carole House: 44:24 Yeah, I love you because that was totally a huge issue that I wanted to talk about. And also on the scale point that you mentioned, and I know this hits on a lot of the stuff that you framed for us, it's scale on sophistication, speed, reach, amount, scaling just in every possible way. And ultimately because of the issue that we talked about before about it being ineffectual. I mean there's a massive effort right now underway where the government has been very clear in messaging that the RFIs that are coming out asking for information on cost. And I do think that the questions that came in were very much an over calibration on questions on cost and not on effectiveness and goodness. This is the precursor to deregulation.

45:12 What's needed is a refocus on effectiveness and there should be reduction of burden and there's massive opportunities for reduction of burden. But I'm not seeing the paired with it true rethinking on scaling effectiveness. And that's where, again, that strategic connective tissue, it's got to be a comprehensive view and vision on all this. And I love the strategic vision that Matt pointed out about this future. Democratic technological primitives being built into the future is totally necessary and I believe in it and we need to push on it. I also recognize that, I believe that's a decades long fight. It's been seven years since we were telling industry in Vienna when we were establishing the fat of standards for crypto when they were saying, "It's impossible to know who's on the other side of the internet." And I'm like, "Not how the internet or technology works." And just, it was basically there's these interesting tensions that are happening between entities that feel that because they're in the tech space, they shouldn't be regulated. And that's on a varied spectrum.

46:14 There's people that also feel that there should be regulation, and then the debate is just around what is that right calibration, where it should be imposed? How do we improve effectiveness and make sure that things are proportional and appropriate and still effective? But there's massive drives for this privacy

movement towards a desire calling for privacy. And even at this privacy summit that I was at, there were a lot of voices that were calling for things so that the core official identity of who you are could never be discoverable and wanting unbreakable privacy and believing that that should be the future in all contexts, including finance. And I would say that I happen to agree with that more so on the tech and information transfer side, I'm more down for that discussion in internet kind of world. The problem is now we've commingled financial and information channels together and finance, this is part of the balancing act of making sure that we don't need a big brother surveillance state.

47:10 But also, and this is where AML constantly gets a bad rap. AML's always painted as the bad guy on things like financial exclusion and also being the only reason why we collect this data, even though there's tons of other reasons why financial institutions collect data in a perfectly private or unbreakably private world. I don't know how you get credit in that future financial system. I'll tell you, I don't know how you deal with civil actions when you want to sue a boss or when you have a contentious divorce, bankruptcy proceedings, if you can't do things for recourse. And then of course fraud. It's a massive issue. So there's a problem of people not looking at these frameworks where they interconnect with each other and where obligations for one thing are reinforced by another. So on your answer about how to scale, I'll say the answer is not firing thousands of regulators and law enforcement.

48:01 And I do think that the answer has to come on the industry side, especially right now given the context towards deregulation. And I hope that it will come with a rethinking and re-envisioning on effectiveness there too and maybe rehiring of people as we recognize that if we have rules, we need them to be enforced, but industry has to be the scale. There's a reason why we put these obligations on financial institutions is so that the government doesn't have to be the recipient of all of this private financial information until there have been certain things that have been determined to be especially useful.

48:31 And industry being responsive and reactive to law enforcement way after the fact, often untimely after the fact, being able to go and conduct two process, which takes time for lots of reasons, things that can scale also better, but that is not going to scale enough. There's a reason why we require financial institutions to have prevention frameworks in place and compliance. So we have to scale that compliance better and help them figure out

how to comply better with a lot of the data and analytics and AI leveraging capabilities that Ari and Matt were talking about.

Ari Redbord: 49:05 Yeah, just quickly, I mean, I think this is the most interesting question, really sort of, I was going to say out there today, but maybe of our generation, right? Post 9/11 we were talking about this issue around privacy and security on airport in airports and on city streets, and today we're talking to them about it on blockchains and across the digital world. How do we ensure that lawful users of technology have a degree of privacy and security in their transactions on a totally open public ledger where everyone can see every transaction in real-time and forever and yet stop bad actors like North Korea from leveraging this type of privacy enhancing technology and taking advantage of the transformative technology. I think that is the question.

49:50 It's been academic for a really long time. I think that more and more we're having pretty real conversations around this, particularly on Capitol Hill as they try to figure out where DeFi fits, if at all, within market structure, decentralized finance, what should be expected of a self-executing smart contract code when it comes to being able to do a lot of what Carole described. I get this question more and more now, "Well, is it possible to do anti-money laundering, AML specifically for DeFi?" And my answer is if you talk to a compliance professional and Matt is one, so happy to have you weigh in. It's a very technical thing. AML involves like a whole host of different types of things, right? Law enforcement response, it involves know your customer. It involves transaction monitoring, policies and procedures, compliance professionals. So my answer is usually, "Look, DeFi protocols today are working with us to do some of that. They're blocking illicit addresses through their front ends. They're members of the Beacon Network." But can they do know your customer as envisioned by the BSA, the Bank Secrecy Act? No, they can't and they shouldn't.

51:00 So I think it's really like how do we figure out how to make sure that we're doing everything we can to keep these growing ecosystems safe, but not giving up privacy that lawful users need in a more and more open financial system? It is tough. I've always believed there are technology solutions to this. Carole speaks super eloquently on this too, but it's like how do we use zero-knowledge proofs to just give enough of what we need rather than create these honey pots of personal identifying information? How do we use digital identity, which is something she's been really evangelized about for years. So I'll stop there.

		But I do think there are technology solutions to all this, but these are really, really hard. I think the hardest questions.
Jo Ann Barefoot:	51:43	In just a second, but one of the things that I hope most fervently for people to think about in this space, especially those working on the regulatory and compliance and law enforcement side, is to get in the habit of thinking about the technology solution first instead of second. Because people default to, "We need a new regulation." "We need a new law." "We need a new best practice protocol." Or something like that. And we do need all of that in many of these areas. But first we should say, could the technology solve a thorny piece of this? So Matt, go ahead and we've got like five minutes left, so I hope you have the answer to everything we've been [inaudible 00:52:35] here.
Matt Van Buskir...:	52:35	I think it will be exciting to do another episode where we actually really get into the weeds of brainstorming this, but it was said earlier, we can't trace our way out of this problem with blockchain. I don't disagree with that, but I also think the answers lie in what we have learned in the blockchain compliance space. If you think about compliance functions before crypto, maybe the number of data points you had to figure out whether someone was a good or a bad actor was sort of your core KYC customer identification program like name, address, SSN, age. I'm going to check and see if my social security number matches this address type of thing when 100% of our identity has been compromised 18 times over. So it's as if it's a real control-
Jo Ann Barefoot:	53:25	[inaudible 00:53:25] held on the dark web by the crime [inaudible 00:53:29] people. Yeah. Go ahead.
Matt Van Buskir...:	53:30	The epiphany I had at Circle, with my colleagues there was when we were forced to figure out how, the vendor we were using it couldn't meet all of our needs because it was made for banking. And when we looked at what the blockchain enabled, it was suddenly turning this away from taking 15 data points and trying to do a binary match to say, "Well, I now have thousands of data points in the cloud and I can put together a data sciences picture and statistical analysis and probability of whether this is good or bad." And when you factor in all of the different data ecosystem capabilities that are out there, this is the solution.
	54:08	I did a presentation to a law enforcement group at one point where I could say, I didn't even need to know the KYC data of a person or where even the money was going. I could look at the behavioral characteristics of the activity and say, "Oh, this

		person is probably buying something for a dark net market based off of the characteristics of their activity." I think the future might be a privacy safe type structure where we're not actually doing the super... I mean, you need to have identities attached to the backend, but maybe those don't need to be shared everywhere. We can actually start to trace the behavioral characteristics of the activity and then figure out how to unlock the identity once we flag the behavior.
Carole House:	54:48	I love this. I promise I'll be quick. Just this was brought up at the privacy thing that I was at where they're like, "It's not identity verification, it's attribute verification." And I'm like, "NIST standards say that identity is attributes combined together in a certain context." I agree. It's really an examination of which attributes should be used in what context, like risk assessment and what should be able to be discoverable or disposable. I think you're totally right.
Jo Ann Barefoot:	55:14	Does anybody have a last word for part one of our conversation?
Ari Redbord:	55:19	I've never done a part two, a sequel.
Jo Ann Barefoot:	55:22	We haven't either on the show.
Ari Redbord:	55:24	Famously, they're not ever as great as the original, so we're going to have, we have our work cut out for us.
Carole House:	55:30	Aliens-
Ari Redbord:	55:30	... for sure.
Carole House:	55:30	Aliens is the best of the entire-
Ari Redbord:	55:32	Aliens.
Carole House:	55:32	Yeah, aliens is an example.
Ari Redbord:	55:34	Empire Strikes back. I know. There are, it has happened. Yeah.
Matt Van Buskir...:	55:38	If you get the four of us talking over beer, I think it's guaranteed to be interesting at least.
Ari Redbord:	55:43	Absolutely.
Jo Ann Barefoot:	55:44	Okay. I'm going to work on that challenge. We're going to do this again. I cannot thank you enough. I have learned so much and

		just been inspired by listening to you all. So Ari Redbord, Carole House, and Matt Van Buskirk, thank you so much for being on the show and to be continued.
Ari Redbord:	56:02	Jo Anna, thank you so much for having me.
Matt Van Buskir...:	56:04	Thank you.