Barefoot Innovation Podcast: Soups Ranjan, CEO, Co-founder, Sardine

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

Jo Ann Barefoot: I have so been looking forward to this episode because my guest today is Soups Ranjan, who is CEO and co-founder of Sardine. Soups, welcome to the show. It's wonderful to have you.

Soups Ranjan: Thanks so much, Jo Ann. It's always a pleasure speaking with you.

Jo Ann Barefoot: We at AIR are doing a lot of work on financial crime and fraud. The problems seem to be a skyrocketing in every direction. We have several projects underway that I'll put information on in the show notes. But you are one of the most expert people that I've ever encountered in really thinking about what's going on and what is changing, where are the risks increasing and what should we be doing about it? How should we be thinking about it? So I'm just absolutely thrilled to have you in one of our first episodes for the new year this year on a topic I know that we're going to come back.

To get started, tell us about yourself and about Sardine.

Soups Ranjan: Yeah, absolutely. So I'm Soups, I'm co-founder and CEO of Sardine. We started the business about five years ago. We say that we are a behavior-based risk platform for solving all risk associated with money movement. So it could be fraud risk, compliance risk, and most recently we also launched credit risk. We have about 250-plus customers worldwide. They predominantly fall in two buckets. One is financial services, so it includes banks, large payment processors, FinTechs, neobanks worldwide. And then the second bucket is online marketplaces, which includes several two-sided or three-sided marketplaces, as well as crypto exchanges, gift card exchanges, et cetera.

And my background before starting Sardine, I used to head risk for companies like Coinbase and Revolut. I'm a machine learning engineer by training, and I have a PhD in EE and an undergraduate degree in computer science. And throughout my life after PhD, I have essentially spent my career essentially fighting different kinds of cyber threats. So first five years were cyber security threats, so working for and helping telcos. Next 10 years was really just helping ad tech firms with click fraud and detecting bots. And then the last 10 plus years have been all around payment fraud.

Jo Ann Barefoot: And when did you found Sardine?

Soups Ranjan: Yeah, we started Sardine five years ago, so 2020, just before COVID hit.

Jo Ann Barefoot: Wow. Okay, great. I remember knowing your name long before I met you, which has been a while now, but you've been such a leader in this space. And so anyway, I'm really excited to have you on the show today.

So we first got the idea of doing this because your colleague Simon was telling me about a presentation that you've put together on types of fraud, and I think there's a lot of challenge for many people in, we kind of use big catch all phrases like fraud and scams, and there's a lot of different things under that roof. So we're going to take a little time at the start and invite you to give us the highlights of how we should be thinking about types of fraud, and then we're going to go into what some of the big trends are.

Soups Ranjan: That sounds like a plan. Perfect. So bear with me one moment, let me just get the deck ready.

Jo Ann Barefoot: And you've agreed to let us put your deck into the show notes, which I know people will be fascinated by.

Soups Ranjan: Absolutely, yeah. Just one moment. Cool. Do you see my screen?

Jo Ann Barefoot: I do indeed.

Soups Ranjan: Awesome. Yeah, so I thought I would spend maybe 5 to 10 minutes talking through some of the emerging fraud and scam typologies we've been saying. So one of the fun things about running Sardine is that customers as well as prospects, they always tell me their fraud stories. So over time, I have essentially become a sort of a custodian of a variety of fraud attacks that people have gone through.

Before I talk to these fraud stories, I just wanted to talk through a few trends that are happening. So one of them is that worldwide, we are seeing that people are demanding and asking for faster payment methods. So UPI in India, Pix in Brazil, in the U.S., FedNow and RTP at various stages of launches. Now we have the saying that faster payments means faster fraud, because unlike ACH or unlike card processing, you have to stop the fraud then and there. Otherwise, when the funds are gone, it's very, very hard to recoup it.

And the second trend that we're seeing is that with generative AI, it's actually becoming relatively easier for anyone to impersonate anyone's identity online, because all our videos and voices are on some social media platform or the other. And it's relatively straightforward now to put it into an AI model and face swap someone else's face onto your face, for example. So therefore, I will posit the question that does rise in deep fakes mean that identity proofing or using identity documents online to verify identities, is that dead?

So here's a video or a GIF showing one of my engineers, so he is actually going through a live ID scan. And what you would notice here is that, Jo Ann, did it remind you of someone, that video? It's actually Tom Cruise. So what he did is he actually superimposed Tom Cruise's face on top of his face. It took him really just two days to generate the whole setup. And the only other thing he would have to do is Photoshop an ID or driver's license, which looks like Tom Cruise, and he could impersonate him potentially. So it's like a live mission impossible.

So now we would actually catch it. The reason we would catch it is because we have this saying that in order to catch such threats, you have to look at intrinsic signals, like how you type, swipe, scroll, move the mouse, hold the phone. And in this case, we are looking for signals which indicate that this was not a real live video screen. It was essentially my engineer had taken over the webcam. So we are looking for signs like when he was doing all of this, was the phone maybe faced down when he did it? Or were there some other things like there was no tap pressure, or was this a real webcam to begin with, et cetera, et cetera? So what we like to say therefore is that the future of ID proofing online will be a battle of bots, extrinsic AI bots, which are trained on your extrinsic features, how you look speak, versus intrinsic AI bots, which is what Sardine specializes in.

Now, we therefore have the saying that no matter the sophistication level of fraudsters, every fraudster has a tell. And so long as you have the data that you've captured, all the telemetry at logins or signups, you can actually oftentimes go back and find out what that tell was. For example, if a fraudster is using a script to create an account online, they may inject mouse movement. However, they may actually forget to add variance, and therefore the mouse is actually just moving in a straight line. So we have signals which look at area of mouse movement, is the mouse moving all over the screen or is it just in a localized area? Or as I was saying, oftentimes fraudsters are renting these device farms where all the devices are in a fixed orientation and there's no shake when you're typing, there's no tap pressure when you're typing. So those are the sort of signals we specialize in.

So yeah, any follow ups to that before I continue?

Jo Ann Barefoot: No, keep going.

Soups Ranjan: So now, I'll walk you through how do fraudsters perpetrate these scams? So a lot of banks, FinTech apps, they are being impersonated online. And in order to actually find, if I for example, I'm banking at Wells or Chase or at a FinTech app like Chime, what have you, fraudsters first have to actually harvest the list of users or the list of consumers who are banking at those banks before they can actually try to spear-phish them.

In order to do that, there are certain loopholes that they exploit. And this is a live example where for one of our FinTech clients, what the fraudster had done is that they were actually typing in different phone numbers and seeing the prompt that came back. If the prompt that came back identified the customer as, hey, go ahead and enter your password, or identified them with a prompt saying, hey, hello Soups, welcome back, then it meant that this customer does have an account with that phone number. So that's what we caught here and we alerted the FinTech to it. The reason we caught it is because we have tools like network graph analytics. Where what you're seeing here is this big blob of phone numbers as you see here. These all the phone numbers which are being entered by the fraudster and the hits are the ones at the bottom here. So I've anonymized the name, so John Doe and so on, and then those are the victims that the fraudster will go after next.

What they will do next is they may actually run a Google ad with that bank or that FinTech's name trying to draw a victim to the fake site, to the fake banking app. Now when you log in into that fake app, it'll look exactly like the real one. So this is what we call spear-phishing. So it'll look exactly like the real app, it'll have the same font, the same UI, et cetera, so you don't even realize that you're in the wrong app. And then the fraudster then takes your credentials and quickly replays it on the real app, and then to quickly replay it, they would use a script or a bot.

Now, where does Sardine come in here is that if the real app, which is the FinTech or the bank was using Sardine, we would alert the banking app that, hey, this is a script or a bot which is actually logging in. As you can see here in this GIF, it is showing somebody is logging in, but the mouse is moving in a straight line.

The next thing that they might also do is they might actually just advertise a fake bank support phone number. They don't even need to recreate a lookalike site, just advertise a fake phone number, and if you have an issue with that banking app, you call up the phone number. And now the fraudster, essentially these are folks actually, unfortunately these are folks sitting in far away countries, India, et cetera, the fraudsters are then going to convince you to install tools like TeamViewer or AnyDesk or Citrix. These are tools which allow the fraudster to take over your screen and to essentially in the guise of helping you with your issue with the banking app, they're actually taking over your screen. They can actually literally blank out the screen when you're not paying attention, and then they can move money out of your account.

Any follow-ups to this?

Jo Ann Barefoot: Are they normally wiping out your account, or do they take money out of it over time, or does it depend on the situation?

Soups Ranjan: It depends on the situation. So oftentimes, they know your password, and then when they have TeamViewer installed on your computer and you have given the fraudster permission to remotely control it via TeamViewer, they can do it whenever they want. So that's the scary part. So my general advice to anyone is to never, ever install any of these tools. These are some of the most sophisticated tools out there that you should never have on your computers on your phones.

And the way we would detect it is that now if, taking Chase as an example, let's say I'm a Chase customer, I have a Chase account, and then if it's my credentials, I'm logging in and it's from my computer, it's from my device ID, my IP address, so Chase will think everything is kosher. However, what's happening is through TeamViewer, a fraudster is going into my computer and then going to Chase. The only way Chase or others can actually detect this is by using techniques like Sardine, where we will tell Chase that, hey, actually a mouse was being moved or the screen was being controlled remotely. Because if our tool was installed in the Chase UI, then we would inform Chase that, hey, the mouse movement looks to be different than what a normal person would do because it's actually being remotely done.

Cool, so moving on, one of the other things that we like to say is these types of fraud attacks are hurting not just banks, it's actually hurting wallets. It's hurting any account which has a store of value. So if it looks like a bank, walks like a bank, talks like a bank, to a fraudster it's a bank. For example, it could be your airline loyalty points. Some folks are sitting on millions of miles, which if a fraudster harvested your credentials, they can actually steal those and redeem them for cash.

The other thing that we like to say is that wherever there's money movement, there are scams. So it's not just for banks. It could be when you're making a rent payment or a hotel booking, or as I said, air travel, et cetera, et cetera. The list goes on and on. The scams have just infiltrated every aspect of our life.

For example, there are Airbnb or hotel booking scams where you might think that you're booking on an Airbnb or hotels.com, but you have to pay attention to the URL very carefully because you could be actually being phished and you're booking on a fake site. Or this is a more sophisticated one, where sometimes fraudsters, they're actually literally taking over the online booking portal at the hotels. Oftentimes at hotels, multiple people who are manning the desk at the hotel, they all share the same computer, they are all logging into it, fraudsters actually phish them. And when they phish them, then they actually install tools like TeamViewer on that computer, and now they can actually start having conversations with guests who have booked at the hotel. And with that conversation, they can do things like, hey, they can say, hey, I had to cancel your reservation. I'm so sorry, you have to make a different payment to me, but why don't you pay me via WhatsApp?

So therefore, any form of payment online that we don't really think about all the time, it can be phished. It could be things like when you're making an airline ticket purchase online, you have to be very careful that you're making a purchase at a valid site, because what we've heard about cases is that you may actually go make a purchase on what looks like a legitimate site. You actually do get a ticket. However, what will happen is that they have added a fake fuel surcharge, because what the fraudster does is they take your card, they actually take the credentials, and then they go and buy the real ticket and they deliver the ticket to you, but now they also add a fake fuel surcharge to it. And they have now harvested your card number and they can go on and make additional purchases on your behalf.

And how Sardine can help in those cases is that if the real ticketing agency, if they were using Sardine, then we would alert them because the fraudster still has to automatically or very quickly make the purchase. So we'll tell them, hey, this is potentially a fraudulent session because they're using a proxy or a VPN, or they're using a script or a bot.

I'll speak to one more example and then would love to hand it over to you, Jo Ann. So yeah, one other example in the similar vein is that it's not just airline tickets, it could be Nike shoes, it could be clothes, it could be what have you. These are traditionally called triangulation attacks where they're harvesting your credentials. Sometimes they're delivering you the actual goods, but now they have your credentials and they can actually do anything with it.

So in short, we like to say that all fraud and scam problems are data science problems, and they can be solved by a merchant or a bank so long as you have gathered the right data. And by the right data, I mean you need to have all the telemetry, like how was the consumer behaving when they were making the purchase? How were they typing, swiping, scrolling, moving the mouse, holding the phone, the tap pressure, the IP address based details? So long as you store all of it, you can go back and find out what was the tell of the fraudster.

Jo Ann Barefoot: Fascinating, thank you. I had heard a lot of those, but some of them I'd never heard that airline fuel surcharge problem before. Oh my goodness.

So we are hearing anecdotally everywhere that scams and other types of payments fraud are skyrocketing, as I said at the beginning. Is that mostly being driven by AI techniques or are other things driving it? What are the main causes and how concerned are you about the trajectory and the risks that we're not going to be able to keep up?

Soups Ranjan: Yeah, no, so they're not necessarily just being driven by AI. So even before AI, we were certainly seeing a rise in fraud. I would say there's a couple of trends. So one is when COVID happened, online shopping just increased, and that did a couple of things. So one is, it sort of made regular consumers also more aware that they could charge back. So what we've also seen is a rise in what I would call friendly fraud. So these are folks who are making a purchase validly, but they are claiming they didn't do it. So that's one trend that we see.

And then of course, second trend we see is because cross-border e-commerce has also taken off. So instead of us buying on shops or websites that are affiliated with our geo, now people are using cross-border e-commerce stores like Shein, Temu, et cetera. And therefore the options available to consumers has become much wider, and therefore it's harder for a regular consumer to know what to trust. So what we're really talking about is trust of which merchants should I really trust. And that's what fraudsters are taking advantage of, because they could set up a lookalike site or they could set up a new site, which looks like legit, but it is not.

Jo Ann Barefoot: Yeah. You touched in your presentation on the increasing inadequacy of our traditional, your customer checks and even the liveness types of checks. Say more about what is the answer to that? If you're a business trying to use those techniques, what are the main things you need to do differently?

Soups Ranjan: Yeah, absolutely. So you definitely need to do liveness, right? So without liveness, I would say any ID proofing doesn't really make any sense, because I could be passing off Photoshop ID. However, even when you're doing liveness, you need to look for not just whether the face on the selfie match the face of the ID, but also look for, as I was saying, are they replaying someone else's video stream? And that is the nuance which I think a lot of buyers are probably not yet asking for. I would urge everyone to be aware that this could be happening. And ask your providers, do they do that check or not.

Jo Ann Barefoot: Okay. Another thing we are hearing a lot about is the theft of records with personally identifiable information, PII, on a huge scale. What should we know about that? How are these breaches being exploited? How can organizations defend against those situations?

Soups Ranjan: Yeah, absolutely. So with rise in theft of PII, I think that there are some novel approaches out there, which a lot of companies are undertaking, which is you got to encrypt all of the data, salted, double-salted, what have you, so that even if a fraudster did get hold of the data, it's actually already encrypted. That's the only solution out there. Anyone who is storing any sensitive data, we have to be very cognizant of that.

And the second consequence that it has to KYC providers like us and others is that because of all the data breaches, a lot of stolen SSNs are floating around, it's actually relatively easy for someone to impersonate anyone, because they have the phones, as they call it, name, address, date of birth, SSN, and all of that stuff, and they can actually verify anyone's SSN online. So I think the key here is to not just blindly look for whether those four pieces of information they match or not, but also look for other telltale signs. It could be triangulate the SSN identity with telco identity or with social media or with phone number identity or bank identity, et cetera. Because even if somebody found my information in a breach, they won't be creating an account online using my phone number. They won't be using my email, they won't have access to my bank accounts.

So I think the bar to doing a really solid KYC online has increased quite a bit, and you got to actually triangulate across multiple data sources.

Jo Ann Barefoot: Yeah, I've been thinking for probably 10 years that the regulatory requirements on how to establish the know your customer to meet the criteria have been completely inadequate for years and years. I mean, it's just the starting point. You have to do all this other work, because it's all for sale, isn't it? I hear people talk about crime as a service, criminals being able to buy techniques and records and everything on the dark web. Is that a rampant problem?

Soups Ranjan: A hundred percent, yeah. So all these tools that I was referencing, for example, there are tools out there that you could purchase which do that quick replay of your credentials. So you don't even have to write a sophisticated piece of software to do it, you could actually buy it off the shelf. You can of course buy identities off the shelf, that's very well known, but you could buy all these sophisticated tools as well very easily.

Jo Ann Barefoot: Well, let me go back to the point you made about encryption. How widespread is the practice of being sure that these kinds of data are being encrypted when they're moving? Is that becoming the norm? Is it still only being done by the most sophisticated companies? Where are we on that journey?

Soups Ranjan: Yeah, I would say it's quickly evolving. I know several companies out there who specialize in, I would call just data vaulting. As these data leaks were happening, everyone rushed into just buying more cyber insurance policies to protect against breaches. However, that doesn't really help you. That's really going to protect you in the case there's a breach.

Then there were a crop of companies which got started, which basically came in and said that, hey, no matter what PII data you have, we shouldn't really think of card numbers being PII. We should think of account numbers for ACH, we should think of SSNs, or we should think of phone numbers. All of those things should be considered as PII and we should just vault it.

Jo Ann Barefoot: Could you define that?

Soups Ranjan: Yeah, what I mean by that is that you should be able to encrypt it and store it, or you could actually segregate the two things. So you could hire a company which does the encryption for you. So therefore, even if your premises are breached, even the encrypted data won't be found because it's lying somewhere else. And you have to just make in your day-to-day use case if you're a bank, and then you have to find that information relevant to a user, you just make an API call to that vault service.

Jo Ann Barefoot: How concerned are you about the advent of quantum computing being supposedly able to break encryption in the near future?

Soups Ranjan: Yeah, a hundred percent. So yeah, given what Google was able to achieve recently, I think it is definitely in the realm of possibility. I haven't kept up to date or I haven't been actually following very closely, so I would be really concerned when that day arrives. But my hope would be that all the cryptography experts out there, they're able to figure out some other algorithm which even quantum computing cannot essentially break as easily.

Jo Ann Barefoot: It's such a dynamic area. I know it's an arms race, isn't it? It's just a constant improvement among the fraudsters, and then the financial companies and law enforcement and companies like yours have to figure out how to get ahead of them.

On the topic of encryption and more broadly, you've touched on this a couple of times, I know your view is that part of the bigger set of solutions on this is that we need to enable more data sharing among the, I'll call them the good guys, the industry, governments and so on. How should the system work? And I think, tell me if you don't agree with this, it seems like the primary obstacle to more data sharing is concern about keeping the data private and keeping it secure. And also sometimes protecting the fact that there's an investigation going on that people don't want to tip off that there's something underway.

So talk about the vision that you have for moving to a system where we can have more data sharing and what needs to be done to be sure that that can be viable.

Soups Ranjan: Yeah, a hundred percent. So there are I would say broadly two ways that people approach the problem of data sharing. One is you take the approach that I will encrypt all the data. So if company A and company B, they want to share data with each other, let's just say they are sharing phone numbers of bad actors or fraudsters. So then the phone number will be encrypted, and if any other company wants to query for whether a phone number is in this block list, even the query would be encrypted with the same technique and then you see if there's a match or not. So that's like achieve using simple hashing algorithms. It works, but it does not allow you to do things like do fuzzy matching, because the phone number has been... in the sense that phone number is the wrong example, but let's say if I wanted to see if a particular name was blocklisted, then I actually want to do fuzzy matching because I may have misspelled the name. Or my real name is Supranamaya Ranjan, I never really use it, only legally I use it, but most often I use Soups Ranjan. So if I wanted to fuzzy match between the two, I can't do that if I encrypted it already.

So what I'm getting to is that there's a trade-off between accuracy and the desire to make all data be private, and we think that there is an optimal path there. I'll get to that in a second. The approach that we have taken at Sonar is that we first want to build the actual use case of data sharing. So we're working with banks and FinTechs, crypto exchanges, et cetera, to enable this data sharing. At the beginning, we're doing it in the clear text, because we can enable things like fuzzy matching. And after we have proven the use cases that yes, these are the use cases we want to support, then we can go back and identify what are the right algorithms out there that can be used to even maybe do this in a more privacy preserving manner. But at the moment, we took the other approach, let's actually first identify the use cases. And then to do that, you have to do with clear text, right?

Jo Ann Barefoot: Is there a need for standard setting and best practice sharing? I guess one thing that always worries me in this space, I mean we have organizations like FATF and the big payments networks, and there are plenty of people working on all of these challenges, but I wonder whether it's hard to figure out how to scale up solutions as rapidly as possible. What thoughts do you have on that?

Soups Ranjan: You have a very valid point. Our thought process here is that this data sharing has to be done at a nationwide level and even across nations. In fact, the approach that Ravi Loganathan, who runs our consortium, we call it Sonar, he often says that we are building Sonar as a national scale utility where we want everyone to use it. We have actually created a different company or an entity for Sonar, which Sardine is a participant in it. And in order to scale it, you have to essentially do it at that nationwide level. What we would love to see is if the regulatory bodies in the U.S., I don't know which ones, combination of FinCEN, OCC, et cetera, they came out and said that, hey, in order to fight these scams, we need all entities to, in the money movement flow, when you're making a Zelt payment or using Cash App or using FedNow or RTP, everyone has to query the reputation of a counterparty against a consortium.

That is what we need someone to come out and say, because only then would people say that, yes, this is important. But otherwise what ends up happening is that all banks, all FinTechs, they think their that data is better than everyone else. And consequently, everyone suffers, because we have to go through several cycles to convince them that, hey, it's in your best interest as well. Otherwise, everyone keeps hoarding their data, thinking their data is valuable, they don't want competitors to learn from themselves. But then as a result, it's the actual consumer who's being hurt, right?

Jo Ann Barefoot: Yeah, that is one of the things I really worry about. I did some work on the AML compliance picture when I was at Harvard as a senior fellow a few years back, and it's the most expensive compliance realm for the financial industry. It's probably more than half of the compliance cost compared to all the other consumer protections and all the other requirements that they have. And yet, it's so inefficient the way we do it now, every individual institution is going through the same processes, they can't rely on what anybody else has done, and sharing is so difficult. There are some mechanisms in the U.S., as you know, for sharing data among banks and with the government, but they are really limited. Is AI part of the solution to this, do you think? And what ideas do you have on that front?

Soups Ranjan: Yeah, no, absolutely. So AI is, I would say, not necessarily a part of the solution for data sharing. We think AI is very helpful for automating manual repetitive tasks. So for example, generating SAR narratives, or if you are filing a dispute to a chargeback, then you can automate that. Or if a compliance agent is actually reviewing a sanctions case or negative news or what have you, then you can actually have Copilots which automate all of that. That's what we provide at Sardine as well. However for data sharing, I think traditional approaches are sufficient.

There are some sophisticated technologies known as homomorphic encryption, which is what we would need to have more breakthrough in in order to achieve optimality around privacy preservation, as well as optimal data sharing. So remember when I was talking about, hey, at Sardine/Sonar we took the approach that let's share all the data in clear text. Less privacy, but more accuracy. The other approach, let's just hash everything, less accuracy, more privacy. But with techniques like homomorphic encryption, you can achieve an optimality between those two trade-offs. But when I last looked at homomorphic encryption, it's not ready yet, because it takes a lot of time encrypting things and doing the computations. So we need much more breakthroughs in that technology right now.

Jo Ann Barefoot: Correct me if I'm wrong, but my understanding of homomorphic encryption is that the data is encrypted and then remains encrypted as you share it with the other party. And if someone does get hold of it, they are not able to decrypt it.

Soups Ranjan: Exactly. The idea is that you could still do a lot of those fuzzy matching even on the encrypted string. So imagine Soups Ranjan and Supranamaya Ranjan, if I encrypted both of them, but you should still be able to do some sort of a fuzzy matching thing, these two names are similar, sort of similar, and come up with a score using a homomorphic encryption technique.

Jo Ann Barefoot: And do you have any sense as to when you think it will be ready?

Soups Ranjan: I don't quite, because I haven't kept up to date with that research.

Jo Ann Barefoot: A lot of things are moving quickly.

Soups Ranjan: I have looked at a lot of startups which were doing this because I was investing in this space quite heavily once, but it's hard to cut through the noise, because they will claim that they're doing homomorphic encryption, but then you look underneath the hood and then it's really just hashing underneath the hood. And I'm pretty sure that there's a lot of great folks who are working actively in this space, so we will have some breakthrough very soon.

Jo Ann Barefoot: That's what I hear as well. I know we're going to run low on time, I would love to hear your advice first for, you've mentioned a few things you think the government should be thinking about doing. Do you have any other advice for regulators or entities like FinCEN, both in the U.S. and elsewhere, that are trying to win this race?

Soups Ranjan: Yeah, absolutely. There's a couple of things that I think would benefit us quite a bit. So for example, with all the SAR data that FinCEN has, that is where we could actually use AI. So right now, of course, under the same regulatory regime of, whatever, if it is GLBA or 314(b), under that if I could query that database if I'm filing a SAR on someone and query FinCEN's database, it tells me a few things about this individual that I'm about to file a SAR on. Because right now, it's a black box. I file a SAR, I may or may not hear back from law enforcement. But me as a bank or Sardine as a vendor serving a bank, I may want to know more details because it helps me as well in my own investigation. And that is where maybe using LLMs or other techniques on that data and providing me with some information, I don't want to know everything, would help all of us. So I think that could be one idea that I've always had.

And the other thing, the time that I've been to Smoke Tree, the thing that was eye-opening to me, Jo Ann, was that regulators or supervisors, they are in as much of a need for better tooling and better maybe AI tools or machine learning tools as banks or FinTechs as well. So you use the word SupTech for that. So in that sort of vein of SupTech, in that world of SupTech, I think one of the things that we could do better is really all the tools that we are selling into FinTechs and banks, actually supervisors could also adopt it. Maybe supervisors could do network link analysis on all the entities that people have filed SARs on. Maybe they already have some tools, I don't really know because I haven't interacted with them enough, but I'm sure there's room for better and better tooling with the advent and AI and ML, right?

Jo Ann Barefoot: Yeah, there are tools that are improving, but I'm into that. That's my favorite subject, helping the regulators get better technology themselves at FinCEN too. And there are a lot of people working on these things obviously, but there's so much more that can be done.

Okay, so that was advice for the government. Do you have advice for companies, banks and financial companies that are in this space defending against frauds and scams that we haven't already?

Soups Ranjan: Yeah, I think just sort of paraphrasing what I've said throughout the show is that, it's important to actually capture the data ahead of time because every fraudster has a tell. So even if you don't necessarily make use of that data right away, the most important thing in fraud prevention is to have the data at hand. So therefore, invest in better tooling, technology, et cetera. Use Sardine, use any other tool like Sardine, but you gather the data, have it in place so that you can actually detect it later.

The second thing I would say is that, when it comes to fraud, I would say people have invested a lot, but scams are still very quickly evolving. And that's where I would love for banks to be more proactive, not just at reimbursing victims post-hoc after a scam happens, but how can you actually prevent the scam from happening? So more proactive approaches, that'll help the consumers everywhere.

Jo Ann Barefoot: Yeah, we've been looking a lot and may do some work on the [inaudible 00:44:54] scam problem, and I know we hear from banks how frustrated they are, because sometimes they are flagging something and saying to their customer, we're concerned that this is not a legitimate thing, but if the customer decides to do it, it's not within the bank's control to block it. That's a really tough situation, but maybe getting better at how to catch and communicate and inform people.

Soups Ranjan: I know, and actually that's a very valid point. For example, for all of us who have elderly parents, if my family was being scammed, I would want to know. So maybe one approach that banks could take is that if my dad is showing up and enjoying loads and loads of cash at ATMs because he thinks he's helping IRS or whoever, inform me, that's the most basic thing they could do, and then I can go and talk to him, right?

Jo Ann Barefoot: Yeah, I think there's a lot of work to be done in that area. AARP in the U.S. does a lot of work on, they like to emphasize that these are not just attacks on seniors, they're attacking everyone, but there's a lot of targeting of senior citizens for these kinds of scam attacks of all stripes. And yeah, should we be doing more to encourage families to set up those kinds of controls at some point, especially as more of our population is aging?

Okay, last question, other than if you want to add anything else, what is your advice to the consumer, most important advice on how to protect ourselves?

Soups Ranjan: Oh, yeah. Be paranoid, right? If someone calls you up trying to sell you something that sounds too good to be true, it's probably not good. And if you feel like you're being rushed into something, don't fall for it. And of course, the other thing being use stronger passwords, use a password manager, use second factor, SMS, but if you can adopt authenticator apps, et cetera, that's even better than SMS. So those are the pieces of advice I have.

Jo Ann Barefoot: Am I right that once people have been scammed, that the criminals start selling their name and contact information to each other, so they're more likely to have more people try? I've heard that.

Soups Ranjan: Yeah, I have not heard about it directly, but that does sound like in the realm of possible things. Yes, definitely.

Jo Ann Barefoot: Anecdotally, I have seen that happen to people around me. I was in an Uber not long ago talking about some of the work that we at AIR are doing, and when I got off the phone, the driver told me about having been repeatedly victimized by scams, and it was really inspiring. He said, "Keep up your work. I hope you have success." Because he had really, really had his life harmed.

Soups Ranjan: Oh my God.

Jo Ann Barefoot: Terrible.

Soups Ranjan: There are a lot of scams targeting Uber drivers as well.

Jo Ann Barefoot: Are there?

Soups Ranjan: Yep. I actually had a slide on it. So it's basically, you pretend to be a rider, basically call an Uber, but then you cancel and then you find the phone number of the driver. And then that's how you then start contacting the driver, and then you pretend to be Uber contacting the driver, and then you pretend that you have to actually, the driver has to give money back or whatever, and then that's how you actually scam them. Yeah, it's pretty rough for them as well.

Jo Ann Barefoot: One more question, even though I said that was the last one. Do we have a good handle on the profile of the criminals we're talking about here? I know many of them are international, I know many of them are running call centers now. They've got bots, obviously. Is there anything that people should understand about who the attackers are? I understand sometimes trafficked people are being forced to operate in the call centers. What's the portrait of the attackers that we know?

Soups Ranjan: Everything that you mentioned. So a lot of these scams, they started being perpetrated by call center folks who worked at call centers, like BPOs, in the off hours they would scam people. Then of course, we've also all read about all the pig butchering attacks that are happening, where folks in Southeast Asia are being coerced into doing these pig butchering scams, and these are trafficked people as you mentioned.

Of course, every geography has its own sort of special typology. You go to Brazil, and even London, there's a gang of folks who are stealing phones. And in Brazil, I've heard cases where they would actually, as soon as Pix was launched, they would actually steal your phone and put a gun on your head and ask you to move money out of your phone. So what we hear people are doing in Brazil now is they carry two phones. They have two phones. So they leave the real phone with financial apps at home, and then they walk outside when they go out with another dumb phone essentially.

And the same thing is now happening in London. In fact, my phone got stolen in London. I was just walking around outdoors and I actually was on a call with my co-founder. I had my phone in front of me because I was looking at Google Maps and suddenly just came, and then they swiped my phone off my hands. And then luckily in my case, I had my laptop so I quickly changed all my passwords. I locked my phone and all of that. But when I did the research, I found that in London also, there's a criminal gang which just steals these phones and they just resell them.

So yeah, so every geo has its own local thing going on. But yeah, scams have just skyrocketed everywhere in the world.

Jo Ann Barefoot: Soups, is there anything that we haven't talked about that you want to add?

Soups Ranjan: No, I think we covered pretty much everything. All I would say is scams and fraud are quickly evolving. So if anyone who's listening to this wants to reach out, maybe we can help you as Sardine, as a company. Or if anyone wants to just jam on fraud, I'm all open to that as well.

Jo Ann Barefoot: And where can people find Sardine?

Soups Ranjan: Yeah, so very easy, our URL is sardine.ai. And you can also find me on, I'm constantly tweeting as well as posting on LinkedIn. So if you just search my name on those sources, you can connect with me there. And my email is also very easy, soups@sardine.ai.

Jo Ann Barefoot: Right. I invited you to speak at an event I hosted at Harvard years ago and you didn't come, and I was so disappointed. I didn't know you, I just knew your name. I'm so glad that today we've been able to share your insights with this audience. It's just fantastic. So Soups Ranjan, thank you so much for being our guest today. It's been fascinating.

Soups Ranjan: Thanks so much, Jo Ann. I really enjoyed the conversation.

Jo Ann Barefoot: Thank you.