FINTECH ONE-ON-ONE PODCAST – SOUPS RANJAN

Welcome to the Fintech One-on-One Podcast. This is Peter Renton, Chairman & Co-Founder of Fintech Nexus.

I've been doing these shows since 2013 which makes this the longest-running one-on-one interview show in all of fintech, thank you for joining me on this journey. If you like this podcast, you should check out our sister shows, PitchIt, the Fintech Startups Podcast with Todd Anderson and Fintech Coffee Break with Isabelle Castro or you can listen to everything we produce by subscribing to the Fintech Nexus podcast channel.

(music)

Before we get started, I want to talk about our flagship event, Fintech Nexus USA, happening in New York City on May 10th and 11th. The world of finance continues to change at a rapid pace, but we will be separating the wheat from the chaff covering only the most important topics for you over two action-packed days. More than 10,000 one-on-one meetings will take place and the biggest names in fintech will be on our keynote stage. You know, you need to be there so go ahead and register at fintechnexus.com and use the discount code "podcast" for 15% off.

Peter Renton: Today on the show, I'm delighted to welcome Soups Ranjan, he is the CEO & Co-Founder of Sardine. Now, Sardine is a super interesting company, they are focused on the fraud and compliance space, they started off in the most difficult part of this space in crypto and we talk about that. We talk about the challenges, the different types of fraud that they're seeing today. You know, we talk about obviously what Sardine offers and the types of products they have, we dig into the weeds a little bit and go and discuss how they're actually combating fraud, you know, we talk about where fraud is coming from, who they're focused on when it comes to onboarding new clients, we talk about real-time payments and much more. It was a fascinating discussion; hope you enjoy the show.

Welcome to the podcast, Soups!

Soups Ranjan: Happy to be here, thanks for having me, Peter.

Peter: My pleasure. So, let's get started by giving the listeners a little bit of background about yourself. You've been at some pretty major fintech names in your career, Revolut and Coinbase, just to name a couple, so why don't you just hit on some of the highlights of what you've done before Sardine.

Soups: I spent about four years at Coinbase from 2015 to 2019, I was heading up risk for them which meant fraud as well as internal tooling for the compliance teams as well as data science. And after Coinbase, I went to Revolut, I was heading financial crime for them globally initially and then later also heading crypto for them and Revolut is where I met my two Co-Founders, Aditya or in short we call him Adi as well as Zahid and that's where the idea for Sardine came from.

Peter: Right, okay. And so then, tell us a little bit about that, what did you see, tell us a little bit about the founding story there.

Soups: Yeah. The founding story is the following. Even if you go back to my time at Coinbase, I don't come from payments so at that time I didn't come from the payments background. Prior to Coinbase, I had spent about ten years fighting other kinds of security-related issues so I spent like five years in cyber security and five years fighting click fraud, right, in advertising. And in a lot of ways my career has been all about applying machine learning and data science to fighting cyber security or click fraud and now it became payment fraud. So, when I look back upon my initial days at Coinbase in 2015 when I was given the goal to reduce fraud rate, I had to come quickly up to speed on, you know, what does ACH mean, what does the….all the various jargons in the banking and the credit card industry, etc. and at that time I realized that, you know, no one really teaches you fraud prevention in schools.

So, I got a bunch of other fraud leaders together and I started something called the Risk Salon which is essentially like a meet-up which all the meetings were held under the Chatham House Rules that you can say what you want to say without attributing it to the source. So, we got together, fraud leaders from all sorts of companies in the Valley, grew very quickly over the next three years to about 4,000 members and I learned a ton from that. Now, fast forward to Revolut, when I went to Revolut, again, one of the reasons I went to the UK was because I wanted to learn about the international payment methods.

So, at Coinbase I thought that I was surrounded by folks who were very much on the let's chart a new territory, create a new financial ecosystem so I learned a ton about the new world which we are trying to build, but I didn't have a good understanding about that old as much, right, and therefore I purposely chose to go to Revolut to learn about all the international payment methods, (inaudible), FasterPayments, etc. And though when I met Adi and Zahid one of the interesting moments in our career at Revolut was that Adi was in charge of launching Revolut in the US so when we were launching Revolut in the US…. we came from the UK so we wanted to be a little more risk averse.

So, we wanted to launch Revolut in the US while enabling 3D Secure whenever you're loading money into a Revolut wallet in the US because you showed the liability and therefore you don't really need to care so much about fraud prevention, but the conversion rate went haywire. It was like and this many low, like 30-ish/40-ish% so the UX was terrible, right. So, those are some of the seeds that, you know, were going on in our heads, right, like to has to be easier for fintechs to launch, it has to be easier for fintech entrepreneurs to grow and scale without actually worrying about fraud or compliance.

So, when we started Sardine that was our motto, that was our goal that, you know, a fintech entrepreneur of today should not have to go through what I had to go through, right, from my time at Coinbase learning up quickly all these things. It should be much easier and they should really just focus on their idea, and product market fit and leave the hard, heady fraud and compliance issues to a company like Sardine.

Peter: Right, got you, okay. So, I've got to ask you, why did you call it Sardine and is there a story behind that name?

Soups: Oh, yeah, there are a couple of stories. So, the name Sardine stands actually, the first three letters SAR, it's Suspicious Activity Reports.

Peter: Ah, right, yeah.

Soups: Yeah. And you find the SAR whenever there's a fraud case in the US about $2,000 or whenever there's a suspected money laundering, right, and the second reason is that it's fishy (Peter laughs) so therefore you can make a lot of memes out of it and it's also easy to say, right. You don't have to struggle with pronouncing it or spelling it, you can say it in a loud bar and people get it immediately.

Peter: (laughs) Right, okay, fair enough. So then, let's just take a step back for a second, when you look at the landscape today, both here in the US and internationally then, what are the biggest fraud and compliance challenges that we face here in fintech?

Soups: A couple of thoughts, on growing trends. So, one is scams, right, so we increasingly like to say that, you know, as faster payment methods take off, like Zelle already and then soon, FedNow, RTP, etc., so with faster payments come faster fraud, right, or scams. And as you probably saw in the UK as well, the dollars lost to scams has actually overtaken the dollars lost to credit card fraud, right. So, we are very concerned that folks are not at all prepared to deal with the amount of scams that are coming our way, right, and money moves very quickly, there's no recourse built-in into any of the networks like Zelle or RTP, etc. These scams, they take multiple forms, right, there's the classic text support scams all the romance scams as well as the brokerage or crypto investment scams, and then another form recently has been what is called the "pig butchering scam," I can explain each of them.

Peter: Right, yeah, please do, please do.

Soups: So, a romance scam would be you get befriended by someone, you start caring for that person, you think they really exist but they don't and then over time, they get money out of you which you keep sending via wires so that's classic. Tech support scam would be you are searching the Internet for, you know, some issue that you're having on a computer, it used to be classically Microsoft Tech Support or used to be Norton Antivirus. But nowadays it's taken the form of, you know, you're in Amazon or Instacart Tech Support, right, like hey, why did my grocery delivery not arrive or what happened to my delivery from Amazon. You go online and you try and search for a phone number for Amazon except you get advertised a fake phone number set up by a hacker, other delivery mechanism is you get a text from what appears to be Amazon except it's not Amazon.

And you click the link and you think that you are headed to Amazon's site but it's a lookalike site, right, and then you get phished essentially, you enter your credentials, then your user name/password, even your 2FA token except you're entering it in a lookalike site. And then the attacker quickly takes the credentials and recreates it over on the other site and takes all your money, right. The other nefarious one that we've seen is that, you know, the attackers often tell them hey, Amazon owes you a refund for an order but in order for us to give you the refund, you first have to send me $100 of Bitcoin.

So, we've seen people being socially engineered into actually going to a physical Bitcoin ATM and it's surprising how many people fall for it and it doesn't click in their head that why would Amazon want you to actually visit a physical Bitcoin ATM and send me Bitcoins, right. But then people do fall for it because there's the psychological element here of greed, right. Or they go to like crypto onramps like Sardine, then they go to MetaMask and they buy crypto except they think they're sending it to Amazon but they're sending it to the scammer, right. There's another one which I actually forgot, I say it's very fastly growing in popularity, it's called Zelle scams or the Zelle Refund scams, right.

Peter: Right.

Soups: So, the refund scams are your bank, all of a sudden, emails you or texts you, calls you saying hey, we owe you a refund, but in order for you to get the refund you have to verify you are who you say you are. And they again take you to a lookalike website or, in fact, they will guide you to the actual bank site as well and then in this case they will install tools like TeamViewer, AnyDesk or Citrix. These are remote desktop screen sharing tools. So, they install this tool on the victim's computer, they can then guide the victim through the motion of going to the bank site and actually convincing them, you've got to send money somewhere else before the bank gives you a refund and all this time they're controlling the screen or guiding the user through the process.

Peter: Right. So, those scams feel like they're really social as much as technological in nature, right, so the technology piece, I'm sure you've got nailed. I'm just curious, before we move on, the social piece seems like a really difficult challenge to overcome.

Soups: The social piece is actually more about education, right. The other element here is, you know, I'm increasingly realizing that all these scams, if you think about, they have nothing to do with the (inaudible) change or with Amazon for gift cards or they have nothing to do with the banks, right, all these institutions are being literally just used as a vehicle. The real issue at hand is that when you get a text message or a call from someone, you don't really know who they are, that was before, right, you can't really….I don't really trust anyone who calls me anymore or texts me anymore because you can easily spoof someone's phone number nowadays very easily and there's a fundamental issue.

The fundamental issue is that when the Internet was built, right, so all the Internet protocols that you look at like Sift for Internet telephony or emails or SMS, etc. they don't actually verify the senders at all so that is the fundamental issue so you can no longer trust where the message is coming from. There's only one country which actually, as of last month, which passed a regulation which is Singapore saying that whenever someone is sending a text message in Singapore, if they have not registered with a central authority in Singapore then you as the recipient, when you get that message, you will actually be shown that this message is coming from someone untrustworthy and it could be a scam or a phishing message. So now the onus has fallen and all the scammers have to suffer the strain and all the telcos have to comply with it. So, that is the sea level change we need, right.

Peter: Right. I think I get texts so much everyday these days that look like they're scam texts with, you know, your UPS package has been delivered or whatever it is and they want you to go and click on something and it's a major problem. But, anyway, I want to talk about Sardine now for a bit so tell us a little bit about what it is you guys do, what are the products you offer?

Soups: So, Sardine is all about behavior-based or behavior-infused fraud prevention, KYC, AML compliance as well as payments. Behavior-based in the following sense that, you know, you had a lot of fraud prevention companies built over the past because fraud is as old as money except all these fraud prevention companies, they were built for let's say e-commerce, right. So, when you're trying to solve for e-commerce fraud you look at shipping address and shopping cart and you can, for the most part, get away with it, is the person who entered this card, are they shipping it to a drop shipping PO box or they just add like the highest value goods into the shopping cart.

But now when it comes to financial institutions like fintechs or neobanks or crypto or NFT platforms or gift cards, etc., right, whenever you are adding a payment method like a card number or a bank account number to purchase something, you don't have a shipping address in the shopping cart, all you have access to is users' behavior which is how you type, how you swipe, scroll, how you move the mouse, how you hold the phone, all of that.

So, for example, if I, let's say, Peter, I stole your phone number or your card number and I'm trying to purchase crypto on a gift card, I'm going to behave very differently. I'm going to copy/paste your information except if I was using my info it will be auto-filled by the browser or I'll be distracted while typing it. Or in the case of account takeovers, right…. so, if I stole your phone and I know your phone PIN code which is not another classic attack vector then the way I hold your phone when I'm opening up let's say a Revolut or a Monzo app the way I hold your phone will be very different from the way you hold your phone.

So, you hear all about these behavior biometrics and we've built one of the most sophisticated behavior biometrics SDKs out there and we use this device and behavior data to fight fraud at, you know, all sorts of checkpoints. At the time of account opening, we fight identity fraud and at the time of account funding as in when you're loading money into your wallet or purchasing a digital asset we fight payment fraud as an ACH fraud or card fraud.

And then finally, we help fintechs who are card issuers. When they have issued a card, we help them with issuing fraud which is whenever I'm swiping a card let's say issued by Revolut, which is in your name but if I picked it up, I'm going to spend it at a location that you never visit or at an MCC that you never interact with or times of day that you never shop at, right, so we look at those anomalous patterns was well.

Peter: Right, that's really interesting. So, I'm curious about some of the things you talked about there, like the device data and I'm wondering if you could sort of explain a little bit more. I'm thinking about like okay, so is Apple storing the information about how I hold my device and then you will see that somebody else has it and is not doing the same way, I mean, and typing and auto fill, that all sort of thing, I guess how are you comparing it to the authentic person because obviously, you know, if someone's using a bot, that's pretty obvious, I'm sure it's pretty easy to compare. But if it's just a criminal that's typing and doing things, what are the actual mechanisms, how do you detect the fraud?

Soups: We are all about intrinsic behavior so we don't do, at least today, we don't do voice or facial recognition, we don't have face ID like products today, for that we rely on what Apple has. Now, the theory we have is that, and I can elaborate on that theory later and then I'll answer your question, the theory we have is that, you know, extrinsic behavior like your face or your touch ID, right, those can also be stolen, right.

You can be like easily coerced under gunpoint to do stuff, right, and (inaudible) but your intrinsic behavior will never change, right, which is like how you hold your phone. And what we do is we collect thousands of data points via our SDKs like how you type, swipe or how you hold your phone, and we then pass it into our systems that we have been computing your behavior profile using various machine learning algorithms. A couple of caveats I want to point out.

One, we are highly privacy aware in the sense that when you're typing, we are not all interested in the content, we map every single character you type into a random key and in that respect, we are actually, we're like card tokenization providers, where they insert our SDK and that will be still our PCI compliant, right. The other interesting thing is that, like if I look back upon my time at Coinbase like 90% of fraud are charge backs, used to come from fully verified identities and pretty much all the companies, the 200 plus companies that we work with, they came to us even though they had a KYC system in place, right, which means that their current KYC providers, they don't really stop fraud and therefore we realize that you have to really look at the users' behavior when they're entering their (inaudible).

For example, if I enter my Social Security number, I'm going to type it quickly from long term memory, but if I have stolen yours then I'm going to be distracted while typing it, I'll contact switch a lot while looking it up or I'll just copy/paste it.

Peter: Right. That's super interesting and I can see there's all kinds of obviously use cases for that. So, tell me a little bit about who your…you just mentioned 200 plus customers that you have, are these mainly fintech companies, I mean, I can imagine that a huge range of companies would have these needs.

Soups: Yeah, no, absolutely. Actually, before I answer that question there's one other thing I forgot to mention which was like….so we offer multiple products. So, besides our risk platform, we also offer another product which is payments, right, and then the third product is our Risk Insights which is a data consortium. So, the reason we built payments is because when it comes to loading money into a wallet, the hardest part is actually taking care of all the fraud and compliance issues.

Peter: Right.

Soups: So, therefore, we have a fully indemnified payments offering where we take care of all the hard product compliance issues. The first instantiation of it is as a crypto onramp so today, that is live on about 30 different wallets like MetaMask, hardware wallets like Ledger, browsers like Brave and music, NFT companies like Royal or, you know, Tom Brady's NFT company, Autograph. So, in all these places today you can buy 30 plus different crypto assets, Bitcoin, Ethereum, etc. using Sardine and Sardine offers incentives (inaudible) as enough card rails for enabling the purchase.

Instant ACH is our core differentiator offering which no one else has where what we've done is ACH is, of course, batch settled, but we realize that, you know, a lot of providers they ask you to load money via ACH and then ask you to make a buy list but the price of crypto has moved in the meantime, right.

Peter: Right.

Soups: Right, so we allow you to purchase that crypto instantly and in some cases we allow you to withdraw a portion of it instantly as well. So, that's literally putting our money where our mouth is and standing by our fraud prevention environments.

Peter: Right, right, okay. So, we got the crypto use case there, what about outside of crypto?

Soups: So outside of crypto, later this year we'll have our payments offering launching, for funding a neobank wallet as well so, you know, that will enable any neobank, any digital wallet. If they want to use fully indemnified ACH to allow folks to fund, we'll offer that or if they want use card rails to fund, we'll allow that as well.

Peter: Right, right, okay. When you're talking about payments, you're mainly talking about the loading of crypto wallets, is that sort of the main product today, is it?

Soups: Yeah, yeah, today it's crypto wallets, that's right.

Peter: Got you, okay. And then when you're looking at the fraud attempts there, where are they coming from? Are we seeing more organized crime with very sophisticated, more so than just the individual trying to game the system, where is it coming from?

Soups: In crypto onramps, a lot of it is social engineering, some of the scams that we talked about earlier. There's also a little bit of friendly frauds, right, so friendly fraud is essentially, you know, folks realizing what the trade went against them and therefore they claim that they didn't do it and then there's also a very specific type of scam/fraud going on in the crypto world which is that of smart contract malware.

Peter: Right.

Soups: So, basically, I'm sure you get tweeted at by these random AirDrops and if you ever wondered what they are really trying to do, what they're really trying to do is they're trying to get you to connect your MetaMask wallet or any wallet that you use to this random smart contract which is malicious and the smart contract is then going to either A) ask for permission that you wouldn't have otherwise given, like there's a set of permissions called "unlimited token allowance," right, which means that anyone....you can give a contract the permission that any assets in your wallet could be sort of siphoned off by that, right. Or the more sophisticated ones, they don't ask for those permissions, but they hide something, obfuscate something in code, which allows them to essentially do the same thing, and then take all those assets off.

So, now what happens is imagine you interacted with such an AirDrop thinking that you'll get rich from that AirDrop, of course, they naturally give you an AirDrop and you're happy with it, but later when you go and try to buy crypto using Sardine, our onramp, what happens is that the crypto will not really arrive in your wallet, it'll just be siphoned off in the other direction.

Peter: Okay.

Soups: So, we think that there is a big need to build what I'm calling the Verified for Web3 so like attributable allow listed contracts which are good reputation.

Peter: Right, right, got you, okay. So then, when you detect fraud and you're working with a lot of the different wallets, I mean, some of which are decentralized, what are you sending back to MetaMask or to Ledger or whatever like indicating that this is a bad actor.

Soups: In that case actually, so the wallets today, they completely rely on Sardine for KYC as well as the payments, right, so there's no information sharing back. So, we don't share information back, with the wallets, and in a lot of cases they don't want that information to be shared back with them.

Peter: Right. Someone's going to fail the KYC process, right, if they're potentially a bad actor. What is the message sent back to MetaMask that this person's a bad actor and then it's up to them to kind of decide what they want to do with that or how does it work?

Soups: No, neither that. So, we offer like a full widget so in that case a customer who is buying crypto on MetaMask or Ledger is actually a Sardine customer so they are going through a KYC facilitated by Sardine and if there's a failure then we don't share any information back. (Inaudible) The wallets, they've taken the stance that, you know, a lot of DeFi wallets, the reason a lot of them are getting popular is because they're privacy aware and they want to keep it like that.

Peter: Yeah, got you, got you, okay. So, you touched on real-time payments earlier in the interview here and I want to just dig into it a little bit because, as you say, real-time payments, real-time fraud potentially, what is that going to mean? I mean, we already have some forms of real-time payments in the Clearinghouse and Zelle, although it's not pure real-time, what do we have to prepare for when we do? I think it's inevitable that we're going to have a real-time payment system certainly by the end of the decade that everyone is using, so how are you preparing for that?

Soups: Yeah, absolutely. So, one of our efforts which I alluded to earlier, that’s a third product, we call it "Insights" so that is our data sharing consortium. So, the idea there is that there is we'll soon need to have a database of trusted counter parties. For example, Peter, if you're paying your gardener via Zelle, you, of course, have that gardener as a trusted contact, but the rest of the ecosystem should also know that they should trust that gardener, right. So, how can we enable different entities in the financial ecosystem to share like a list of trusted counter parties, right, because on the other hand, if you got scammed by, you know, someone from India saying that he sent me dollars, right, then we want to quickly spread this information across the network such that no one else gets scammed as well.

Peter: Got you, that's great.

Soups: And we are launching this consortium very soon so like in about a month's time. We hired a gentleman named Ravi Loganathan who was formerly the Chief Data Officer at Early Warning Systems so he knows a thing or two about building consortiums, so he is leading the charge for us. We started with about ten founding members, we have about eight identified, the idea would be to set it up as an entity under the Sardine TopCo, but a separate entity and then have all these founding members, they create governance, rules, as well as pricing, etc.

Peter: Got you, got you, okay. A couple of things I want to get to before we close. You know, I noticed you have a pretty impressive cap table with some of the investors that you've attracted here, least of which is a16z. I saw Angela Strange is actually on your board, famous fintech-focused VC, I'd love to know sort of what those conversations are like, how are you leveraging the expertise from some of the people on your cap table?

Soups: Yeah, sure. So, we've been really fortunate, you know, having some of the sharpest minds in this industry helping us along. So, we have on our board Angela Strange, we also have our seed lead investor, Ross Fubini from XYC VC that previously started Village global as well, so he's also on the Board. So, a16z led both our A and the B rounds, and in the B round we also had Visa and in the A round we had Experian and we also have the help of many, many investors, I'll probably forget them all, but a few that come to mind are, you know, Nyca, Activant, Sound Ventures, etc.

Our board meetings are actually pretty interesting so the way I like to lead them is I actually send them a written update which is initially 50 pages long (laughs) about a week before the board meeting. The expectation is that everyone on the Board, we have besides the Board Members we have several observers, they expect that everyone comes prepared having read it and I then just do like a half hour Exec Summary discussion during the board meeting and then we do like three discussion topics.

During the discussion topics, and the topics could be things like hey, how should Sardine diversify into other high-risk categories for fraud product so that was the last discussion topic. And we have a saying now that if you grow up in a tough neighborhood like crypto then you learn a trick or two. So therefore for fraud prevention we are now going into, you know, other high-risk categories, like we already help one of the largest cannabis payments processors for debt fraud, we just signed one of the largest gift card processors for their fraud and we also just recently signed one of the largest well known luxury brand for their digital collectible fraud prevention.

So, therefore, the board meeting, that was one of the topics, what are the adjacent categories we should go after, who can help us and our board members and our investors, they're very fortunate that they all pull up their sleeves and they help us with the ventures. We like to almost see them as part of the company and they help us with a lot of that BD, right, so that's one. The second help is, of course, always Angela and Ross and others they're always available to me as a sort of a sounding board on, you know, any other thorny topics like, for example, the SVB crisis, before that, also how should we be growing the company or the team, what are the gaps, who should we be hiring, etc. So, those are a few that come to my mind.

Peter: I appreciate the color there, that's super interesting, okay. So then, last question, what is next for Sardine, you've got a lot of places you can take this, what are some of the things that are coming down the pipe?

Soups: Yeah, absolutely. So, I alluded to it earlier so number one for our fraud prevention platform, our risk platform, couple of things. One is, you know, diversifying into high-risk categories, right. So, besides the ones that I mentioned, we are also looking into other kind of things like OTA which is travel and then we're also looking into anyone who has a wallet, like any physical retailer, the likes of Target, Home Depot, etc. they all have a close-loop card, can we help them with their fraud? So that's more of a go-to-market diversification, right.

The other interesting thing is that because we built a platform which is one API, one contract, one dashboard for both fraud and compliance teams, we recently signed Stearns Bank as our first sponsored bank customer. And what Stearns is doing is whenever they're onboarding a fintech, right, they have full visibility to give ICA a nod and it's shared visibility between the sponsored bank and the fintech. So, we are taking that approach of, we call it "portfolio view" like this sort of a shared view, portfolio view of KYC. We're taking this approach to other, you know, sponsor banks and other Banking-as-a-Service platforms so you'll see us continuously iterating and developing more features there so that's on the risk platform side.

The payment side, as we discussed earlier, already enable crypto onramp soon later this year, they'll build an API first product which will then enable other use cases like loading money into a neobank wallet so that'll be the second. And then the third is our Risk Insights Consortium, we're going to be announcing it later this year and starting with a couple of use cases, one is sharing data about ACH fraud and then the second is sharing data about counter parties.

Peter: Right, right, okay, great, we'll have to leave it there, Soups, thank you very much for coming on the show, really fascinating what you're building there and best of luck to you.

Soups: Thank you, thanks for having me, Peter, I appreciate the time.

Peter: If you like the show, please go ahead and give it a review on the podcast platform of your choice and be sure to tell your friends and colleagues about it.

Anyway, on that note, I will sign off. I very much appreciate you listening and I'll catch you next time. Bye.

(music)