Barefoot Innovation Podcast: Neha Narkhede, Co-Founder and CEO of Oscilar

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

Jo Ann Barefoot: We have a fantastic show today. My guest is Neha Narkhede, who is the co-founder and CEO of Oscilar. Neha, thank you for joining me.

Neha Narkhede: Thank you so much for having me on, Jo Ann.

Jo Ann Barefoot: We are doing a lot of work in the realm of financial crime and fraud. It seems to just be a skyrocketing topic all over the world, so we're really looking forward to hearing about what you're doing at Oscilar. But first, tell us about yourself? What's your own background and what's the journey that brought you to this work?

Neha Narkhede: My background is in data and AI technology. Oscilar is my second company. My first company, Confluent, makes real time data and AI software. As part of taking Confluent public, I got an opportunity to work with major financial institutions, given how big Confluent's reach was. I discovered that fraud risk and compliance were actually the biggest use cases of data and AI in the modern world. What I identified was a critical gap in the market, which is fragmentation. Point solutions focused on very individual aspects of risk management. They don't just share signals across the customer lifecycle, across products. For example, if you detect synthetic identity risk during onboarding, that valuable signal cannot inform payment fraud decisions at transaction stage. I founded Oscilar to bridge this gap by creating a unified AI powered and real-time risk decisioning platform that provides a more complete 360 degree view of the user's risk profile across the entire customer journey.

Jo Ann Barefoot: Tell us more then about Oscilar? When did you found it? What's the current scope of what you're doing? Then we'll go deeper on the solutions that it's providing.

Neha Narkhede: Yeah. Oscilar was founded a little less than four years ago. What we do is basically provide a complete suite of risk decisioning solutions from KYC, KYB, onboarding risk to credit underwriting risk to fraud risk and AML compliance risk all-in-one platform powered by AI, and our focus is very much pragmatic and responsible use of AI to solve for all this AI-generated fraud that is happening today.

Jo Ann Barefoot: Who are your... Or give us some examples of the types of entities that are your customers?

Neha Narkhede: Our customers range from top 60 banks to regional community banks, top credit unions, fast-growing FinTechs like Dave, Nuvei, Happy Money, and so it ranges quite a broad span of the entire FinTech space.

Jo Ann Barefoot: Are you in the US or global or international?

Neha Narkhede: We started by operating in North America, and I have now expanded Oscilar to the UK and Latin.

Jo Ann Barefoot: Tell us about the name, Oscilar?

Neha Narkhede: Yeah. It's a great question. I get that asked all the time. I thought as I studied more the risk space, risk is never a static thing. It always bounces between two ends of a spectrum. On one side is higher approval, lower fraud. On the other side is lower approval. What I saw is risk just keeps oscillating between the two ends of the spectrum, and so that is why I came up with the name Oscilar.

Jo Ann Barefoot: I love that. Great. Tell us more about how it works? I'm fascinated by this ability to enable the signals to be shared. It has seemed to us for a long time like one of the reasons that the criminals and money laundering people and fraudsters are winning against the good forces to such an extent is that it's very hard to share information in this space because it has to be kept private, it has to be kept secure, and there are so many barriers to flow of the information. How have you solved the problem of sharing the signals across?

Neha Narkhede: Oscilar's technology, maybe I should just explain a little bit about how it works. It works by connecting dots that traditional systems miss because they operate in isolation. Traditional fraud systems look at a very narrow slice of data. Those that do identity verification just look at identity signals at onboarding time or just transaction signals later at transaction time. But simply put, in very simple words, they're like security guards who each watch one entrance without communicating with the other. Oscilar instead creates a unified view by processing thousands of signals in milliseconds, from device fingerprints to behavioral biometrics to transaction behavior histories. We then build unique cognitive signatures, is what we call them, for each user based on how good users interact, so we can then spot the bad ones once we understand how the good users behave. We monitor continuously across the entire customer journey from creating an account to logging in to transacting to also post-transaction monitoring to look for AML.

We share that intelligence across all the touch points of the journey inside the company. Risk detected at one stage informs decisions at the other, which just where reasoning from first principles made all the sense to me. We leverage advanced and explainable AI models to use this shared intelligence, this 360 view, to make well-informed and accurate decisions for all types of online risk problems. For instance, if subtle device anomalies are detected during onboarding when you are creating the account or signing up, that signal is then

remembered and it's factored into the transaction risk decision later. We've actually seen our customers catch 60% more account takeovers using just this approach. This is the platform it adopts to new threats in real time rather than relying on static rules, making Oscilar particularly effective against AI-powered fraud attempts like synthetic identities and deepfakes even.

Jo Ann Barefoot: As the data is shared, do you need to work on encryption and other privacy measures as it's flowing? Because I know that many financial companies, part of the reason they silo information is that they don't feel like they are free to share the AML risk monitoring with the fraud monitoring, even though it seems logical to do so. Within the financial company, is it easy to just share actual identity information and personally identifiable information?

Neha Narkhede: Across the company, yes. The way Oscilar is designed is it's privacy and security first. The way it is designed is data for a particular company does not leave that company's installation to another company. That's one aspect. But even within the company, a user touches different parts of the product at different points in time, and it exposes different forms of risk at each point of time. If that is not using a foundational 360 complete view of who the user is, how do they behave, how does that compare with behavior of good users versus bad users, that's actually a big lost opportunity. That is what is causing very high false positives. It gets in the way of good users, but it's also lowering the fraud detection rate because of all these missed opportunities given fraudsters just break into different aspects of the journey because they know that signals are not shared.

Jo Ann Barefoot: Yeah. Absolutely. The false positive issue is such a huge problem in this space as well as the false negatives as you're saying. Do you find issues arising that relate to the regulatory frameworks, either in AML or in other aspects of what you're doing? Are there areas where we could do a better job against fraud if we had some changes in the regulatory approach?

Neha Narkhede: Yeah. I can give you my view on the current regulatory framework around AI and financial services and whether it's keeping pace with technological advancement or not. But in my view, I think these regulatory frameworks for AI in financial services are still evolving. They face challenges keeping pace with technology as technology is changing so rapidly right in front of our eyes. The current landscape, I think varies pretty globally too. EU's AI Act and the CFPB guidelines in the US are making progress in establishing these guardrails, but there are still significant gaps. Regulators are particularly focused on explainability and compliance, essentially ensuring AI decisioning is transparent, but particularly in credit risk. Now, this creates a balancing act for financial institutions as they need to adopt advanced AI to combat increasingly sophisticated AI-powered fraud, like synthetic identities, while still ensuring that their models remain interpretable compliant.

What we've done at Oscilar is we've designed our platform with regulatory [inaudible 00:11:31] AI, as I call it, from the very start. Our models are explainable, they have full audit trails. We built transparency into the risk

decisioning, so you can always trace back to why a particular decision was made. I think this approach allows financial institutions to leverage this advanced AI for better risk detection while maintaining regulatory compliance. I think the most effective path forward involves a dialogue between innovators and regulators to establish pragmatic frameworks that protect consumers, but without stifling the technologies needed to combat this evolving AI-driven financial crime.

Jo Ann Barefoot: Interesting. The explainability issue is obviously important, but it sounds like it is a limiting factor. The ability to explain things to the comfort level of the regulator may limit the ability to get everything we could out of the tools. Is that true?

Neha Narkhede: That is true for some problems. For credit risk, I think it's completely justified to have a certain level of explainability. That's where fairness really matters. On the fraud side though, it's a little more nuanced. On the fraud side, there are certain fraud problems where it's just really hard to detect them if you just depended on the static rules or the old style machine learning models that are purely predictive. I think we are moving to a world where you need thousands of signals to be processed through multiple algorithms, and only machine learning and AI techniques can do that. Some of them are not explainable. Actually, that's the real dilemma that we face today as things stand today is not each one of those models are explainable. Now you're limited to actually using only those AI models that are explainable to even detect fraud, where some subsection of fraud just doesn't... It's not impactful to use the limited set of AI models.

Jo Ann Barefoot: Yeah. Can you talk to us about what types of fraud are growing most rapidly and why?

Neha Narkhede: Yeah. I think synthetic identity fraud I believe is about 70 or 80% of all forms of fraud, and it is growing extremely fast, especially in Europe. The second, scams. Just social engineering scams are on an absolute rise. They are a huge problem globally, but also in specific geos and the APP account push payment fraud is now on its rise. I would say it hasn't reached the levels of fraud for synthetic identity and scams, but it is absolutely one of the fastest growing forms of fraud given that we are moving to more real-time payments.

Jo Ann Barefoot: Yeah. You just maybe answered what I was going to ask, which was, is push payments fraud growing? Okay. What can you share with us about the solutions beyond detection? Does Oscilar report suspicious activity to FinCEN in the US and so on directly or equip your customer to do so?

Neha Narkhede: Yes. Oscilar has built technology features for 314(a), 314(b) reporting. We enable our customers, the banks, the fintechs, to not only file SAR reports easily, but also report entities that need to be reported for various sanctions, etc., in a single click. That's something that we have done to make things easier. Also, on the SAR reporting side, I think risk operators spend about 80% just sifting through data. Maybe they miss certain data to add it to a SAR report, but we're using a Copilot, a generative AI-based Copilot called Oscilar AI, which just pre-fills everything, saves a huge amount of time so the human can just go in

and review things and then hit submit. There are some very important operational as well as feature-specific improvements that we've done in that zone.

Jo Ann Barefoot: Okay. Great. Do you have a perspective on whether law enforcement is making any headway in getting at the sources of fraud? Your customers have to detect it and either prevent the fraudulent entity from getting into their institution, or if it's already in there, finding the problems that are occurring and reporting them and shutting it down. But when we think about the global trends in this realm, are there things that you think that government could be doing that would be actually creating enough disincentive that we could turn the tide?

Neha Narkhede: Yes. I think we should facilitate secure intelligence sharing when it comes to fraud. Financial crime exploits gaps between institutions, so creating protected channels for sharing these emerging fraud patterns can certainly help the entire ecosystem respond much faster while also maintaining privacy controls. I absolutely think this intelligence sharing network, which is supported by law enforcement, is extremely effective in really curbing forms of fraud because fraud doesn't just impact one organization or one person. That particular fraudster actually goes after hundreds of organization across thousands of users. If one entity had reported it, then at least the other entities could have saved themselves a lot of effort.

Jo Ann Barefoot: Do you have a view on whether the privacy protection capabilities are robust enough to enable that broader sharing? Because that's the thing we always hear about is if you are a bank or if you are a law enforcement entity, you have to protect the privacy of innocent people who may be reflected in data that you would be sharing, and you have to protect the integrity of an investigation if there is one. You have to limit the exposure of that information or encrypt it or do something that doesn't just share it widely. What are the solutions for that today?

Neha Narkhede: Yeah. Cryptography has actually made a lot of progress to a point where the encryption protocols that will be in use, whether you're sharing the data in flight or you're storing the data at rest, those encryption protocols are in place and ready to use if you were to do this kind of intelligence sharing. Think about creating a signature for a particular user and their, let's say, device and not having to share the particular user's PII at all, but just sharing that signature, which is cryptographically generated, that itself will be different for two different devices so those kinds of encryption technologies can be put into effect to actually share it in a data privacy manner.

Jo Ann Barefoot: Interesting. Do you have a view on whether we should be moving toward more digital identity infrastructure as a privacy and data sharing and financial access opportunity? I know I'm pulling you a little beyond your primary scope, but you're so thoughtful on all of the solutions here.

Neha Narkhede: By digital identity, do you mean an API-based verification of diver's license or passport and stuff like that?

Jo Ann Barefoot: Yeah. Probably.

Neha Narkhede: Yeah. Absolutely. I think if we had an infrastructure like let's call it identity verification for driver's license, for passport, that entities could simply call out to and get an answer to. That ultimately is going to curb synthetic identity fraud like nothing else will. That I think if we did that, then we are many steps ahead of the fraudsters. In the absence of that, you have to use many other techniques. You can still stop synthetic identity fraud, but it becomes a pretty big technological investment.

Jo Ann Barefoot: This is fascinating. What have we not talked about that you want to add?

Neha Narkhede: Let's see. I think one thing that might be helpful is how does Oscilar balance the need for this comprehensive data analysis with privacy concerns and regulations on the other hand?

Jo Ann Barefoot: How do you?

Neha Narkhede: At Oscilar, we balance this comprehensive data analysis with privacy through both technical architecture as well as governance practices that we have in place. First, we design our platform privacy by design principles. For example, when analyzing device intelligence and behavior data, we focus on patterns and anomalies rather than PII. Our models are trained to detect fraud signals without requiring excessive personal data. That's one. The second is we maintain strict data segregation. Like I was mentioning, our unified platform connects insights across the customer journey, but establishes appropriate controls on what data can be shared even between different risk functions in an organization. This ensures compliance with regulatory requirements while still enabling this holistic risk view that makes our approach effective. Third and last thing is we ensure all AI models are transparent and explainable. Financial institutions must justify their decisions to both consumers and regulators, so our technology can just provide them clear audit trails of why, when, what happened, and show them exactly what factors influenced each risk decision or assessment. I think the key is treating privacy not as an obstacle, but as a fundamental design requirement.

Jo Ann Barefoot: Are you seeing... As we see the rapid uptake of generative AI in particular today, I know many, many people in the industry are establishing or changing their governance approaches and standards around use of AI. Are you encountering more of that as a line of questions or is it just the normal traditional review of the vendor risk approach that you're going through? It seems like there's two streams of change, one being adoption of new kinds of tools like yours, and the other being this overall focus at many institutions on AI governance.

Neha Narkhede: Yeah. Our bigger customers do worry about and ask questions about our use of generative AI technology and how we're using it, where the data goes, whether that data is encrypted or not. These questions are legitimately coming up and they should. Our smaller customers, of course, have more understanding of the latest technology, so they're less worried about that. But we work a lot on education to our customer base on how we are using that technology. For instance, we don't just paste things in ChatGPT and get answers. Right? That's not secure. That's not a secure way to use it.

You first of all turn on enterprise features in some of these tools that you might be using where they do not actually retain data beyond a certain small window. That's one. The data is encrypted over the wire as you send that using protocols like TLS, and then it is encrypted on rest using protocols like AES-256 and so on. There are ways in which you can use the generative AI technologies that make them very secure, very private, and very practical to use as well. But to answer your question, the questions do come up in our slightly larger and more traditional customers.

Jo Ann Barefoot: Do you look forward, Neha, toward where we're headed in let's call it financial services, risk management and compliance? Your company is at the cutting edge of using data and technology in new and better ways. Do you think that we're moving toward a system in which the risk managers will really have the good information that they need and the good analytical tools that they need to make a big difference in the risk issues facing financial companies and the compliance issues? I worry that we are in a losing race currently where the risks are rising rapidly and most of the traditional tools of both regulators and industry risk managers are not equipped to keep up with those risks because the information is too fragmentary, as you say, too disconnected, too old, too hard to access. Do you envision that we're moving toward a much, much better system in the coming years?

Neha Narkhede: Yeah. Absolutely. I think the vision I had also a little less than four years ago was that the space is moving towards the direction of consolidation, not fragmentation, and the space is moving toward a pragmatic use of AI, not using static rules like we used to. What have I seen in the last four years? Well, Oscilar has grown tremendously fast, so that has been the biggest indicator in my view on whether these two bets are paying off. That is one signal that we see. The second thing is, yes, a lot of the bigger FIs are stuck on technologies that are fragmented that have no idea how to use the late, the greatest in AI. It will take some time to supplement them. It will take some time to update them or remove them. That process is going to take a couple of years, but I absolutely see organizations of all shapes and sizes going after the vision of consolidation and use of pragmatic AI, including generative AI.

Jo Ann Barefoot: Do you have advice for regulators and policymakers as they think about trying to help us move toward that kind of a better model?

Neha Narkhede: Yeah. I think there are some emerging trends that regulators and financial institutions should be preparing for now. There are three critical emerging trends, I think, in financial crime that require attention now. The first is AI-powered synthetic identity fraud is accelerating. Fraudsters are using this gen-AI tools to create realistically-looking fake identities, complete with deepfake photos and fabricated histories. These identities can pass traditional KYC checks, but they actually leave subtle inconsistencies across device interactions, application behavior, which is the silver lining. That is where technology that I mentioned before, like device fingerprinting, behavioral biometrics, if you employ that, then even synthetic identity risk is detectable. Financial institutions need that kind of advanced behavioral intelligence to detect these sophisticated attacks, at least when it comes to synthetic identity, which is huge. The second is cross-channel fraud is growing more coordinated.

Criminals have figured out that there is fragmentation, but there are fraud rings entirely that exploit gaps between different systems in the same organization. Using information gathered in one channel to execute fraud in the other is a really big problem. This is what requires breaking down silos within organizations to create that unified view to not have any regulation come in the way of that. Third is I was mentioning real-time payment fraud. It's surging globally and instant payment systems are expanding rapidly. That's exactly the future of payments that we want. These attacks leave almost no time for manual review, making AI-powered prevention absolutely essential. We are seeing particular focus, sophisticated schemes in regions where real-time payments are well-established, especially in Europe. Regulators and institutions should focus on developing these cross-functional teams and ethos, implementing continuous monitoring capabilities and establishing frameworks for explainable AI that can adapt [inaudible 00:31:13] the speed of these emerging threats.

Jo Ann Barefoot: That is fascinating. Is there anything you want to add that we haven't talked about?

Neha Narkhede: Yeah. I'd like to leave some thoughts or something to share with regulators and policymakers listening to the podcast about how we can all prepare better for the future of financial technology.

Jo Ann Barefoot: Go ahead.

Neha Narkhede: My message to regulators and policymakers would be to embrace collaborative innovation rather than adversarial oversight. The most effective regulatory frameworks we've seen share three characteristics, right? First, they focus on outcomes and principles rather than prescriptive technical requirements. This allows innovation to flourish while maintaining strong consumer protections. A second, they create structured dialogue between industry and regulators early in the development process. When at Oscilar we share our approach to model governance and explainability during the development phase rather than after deployment, it actually has built trust and has prevented costly redevelopment.

The third is they recognize that technology can create strengthened compliance, not just create new risks. Real-time monitoring, automated documentation, explainable AI are all the things that we as vendors can all enhance regulatory oversight while reducing that kind of operational burden. Finally, what I want to say is the fraud landscape is evolving rapidly, and AI powered attacks are becoming more sophisticated. By working together to develop frameworks that enable this responsible innovation, we can actually turn the tables on financial criminals and create a much more secure and inclusive financial system.

Jo Ann Barefoot: I love those points. I want to actually reinforce the point that you made on moving toward principles and outcomes-based approaches, especially outcomes. There's been a debate for so many years between principles-based versus process-based requirements and prescriptive regulation, and they both have their pros and cons. But as we come into an era where there's a lot of ability to measure outcomes, I think we have work to do in defining what does a good outcome look like? Why are we regulating this thing and what do we want to see? Then not care so much about how it's achieved as whether it's achieved, whether we can improve those outcome performance metrics. We don't have a lot of that in financial services because until recently, it hasn't been possible usually to really measure it. But I think if we work collectively, as you say, and collaboratively, we can move toward a better system like that, better results.

Neha Narkhede: Yes.

Jo Ann Barefoot: Yeah.

Neha Narkhede: Absolutely.

Jo Ann Barefoot: That's wonderful. Where can people get information about Oscilar?

Neha Narkhede: Best way to reach us is through our website. There's a form to reach us via or email at hi@oscilar.com.

Jo Ann Barefoot: Okay. Great. Neha Narkhede, thank you so much for being our guest today. It's been fascinating.

Neha Narkhede: Thank you so much for having me, Jo Ann. I really enjoyed it.