FINTECH ONE-ON-ONE PODCAST NO. 402-BENCE JENDRUSZAK

Welcome to the Fintech One-on-One Podcast, Episode No. 402. This is your host, Peter Renton, Chairman and Co-Founder of Fintech Nexus.

(music)

Before we get started, I want to remind you about our comprehensive news service. Fintech Nexus News, not only covers the biggest fintech news stories, our daily newsletter delivers the ten most important fintech stories into your Inbox every morning and we have special editions for Latin America as well as UK and Europe. Stay on top of fintech news by subscribing at news.fintechnexus.com/subscribe

Peter Renton: Today on the show, I'm delighted to welcome Bence Jendruszak, he is the COO & Co-Founder of SEON. Now, SEON is all about fighting fraud and they have a very sophisticated system, we talk about the way their system works, how they are able to catch so many fraudsters, we talk about the different types of frauds, synthetic fraud, account takeover fraud and others. We talk about the different fintech companies that are using SEON today, we talk about the idea that they give away there, some of their fraud tools for free. You can actually go to their website and start using them right now, we talk about the philosophy behind that, we talk about where we are in the fight with fraudsters, whether we're winning, how that's all going and we talk about what might happen in a downturn and much more. It was a fascinating discussion, hope you enjoy the show.

Welcome to the podcast, Bence!

Bence Jendruszak: Thank you for having me, Peter, it's a pleasure to be here.

Peter: Alright, great to have you. So, let's get started by giving the listeners a little bit of background. I know that you're originally from, is it Budapest?

Bence: I'm from Hungary, yeah, I live in Budapest actually, originally, yeah, I'm from Hungary.

Peter: Okay. Tell us a little bit about sort of your story and a little bit of your background.

Bence: Well, I say I'm from Hungary, but actually I don't necessarily think of it as a home per se because when I was growing up we lived in a bunch of places, in a bunch of countries. We lived in Romania, in Russia, in Kazakhstan. All during my primary and middle school years, I was living everywhere and then we moved back to Hungary and started university there and I met my Co-Founder, Tamas, and we were both crypto enthusiasts, this was back when cryptos were nowhere near as popular as they are today.

We actually started building a crypto exchange and we faced a bunch of frauds so people were checking out with stolen credentials and stolen identities after we started accepting credit card payments. We realized how big of an issue fraud is, that was our first touch point with fraud actually and when we looked at the fraud prevention space there were all these providers out there, but they were all aiming for an enterprise sales motion, having to sit through multiple discovery and sales calls,

faced with complex pricing structures, complex integration processes. We felt like we were not their ideal customer profile at that point in time so we said, okay, well our only option seems to be if we build our own tool in-house like a terrible MVP in-house and hopefully that's going to solve our issue on the short term for now.

And that turned out to be a really good decision because we actually pivoted and we started building a massively scalable Software-as-a-Service tool out of it which is fast forward a couple of years, here we are with SEON. We're Series B funded earlier this year, we're 300 full-time employees so it's been a massive journey, it's been a lot of fun.

Peter: What's your geographic footprint? I think we got to know you when you were in Europe, but I know now that you're in the US, like where are you operating?

Bence: So, initially we started out building our core team in Hungary and then we realized Hungary is a small country, engineering talent pool was great, but when it comes to let's say bringing onboard a chief commercial officer we're going to have a hard time finding somebody either from the fraud prevention world with a background having seen fraud and different types of fraud and payments and so on.

But, even broader than that, you know, there's not many Software-as-a-Service companies having been built out of Hungary, So, initially, we kicked off our UK office, we opened it just before the pandemic hit and now, we're about 35 full time employees in the UK. That's where I'm sitting at actually, I'm in our London office just now and I'm moving over to Austin where we have just over ten team members. I think nearing 12 full time team members out of the US and then in Jakarta we have an additional 12 team members. So, 250 in Hungary and the rest worldwide spread between London, Jakarta, and Austin, Texas.

Peter: Right. Austin's becoming a bit more and more of a fintech hub, it seems, I hear a lot of companies that are setting up shop there. So, let's take a step back, I want to just talk about fraud in general, particularly from a fintech perspective, what are the major types of fraud that fintech companies really need to be focused on?

Bence: Well, for one, we've seen plenty of identity theft over the past couple of years. With the wave of COVID, we did see a lot of people being phased out of their jobs, facing economic hardships and therefore, I think, people were just more vulnerable, in general, when it came to, you know, looking at phishing scams, money mill scams. They were being told that were going to be applying for a job offer and in reality, their identities were being stolen in the background and being used to open up bank accounts in their name or even register online for credit applications and so on. So, I think we've seen plenty of identity theft and fraud stemming from that.

But, apart from that, we've seen plenty of credit card fraud on the rise as well. So, COVID in itself fueled consumers to become more immersed in the digital world than ever before, but at the same time, we've seen a greater number of people being faced with the issues of fraud throughout this acceleration of fraud so COVID for us has been an accelerant than anything else.

Peter: Right, okay. So then, what is it that you guys do, I know you're not going to give away your secret sauce, but how are you detecting fraud?

Bence: Well, the funny thing is I'm happy to share our secret sauce, right.

Peter: Okay, then please do.

Bence: If you go on our website, you can register and you can trial it out yourself, we've got nothing to hide. In fact, I believe that's ...in order to move towards a fraud-free world, I truly believe that, you know, you should be able to test out a product before you start using it. You should understand the fully fledged feature offering and the portfolio of products that you can use from that specific company. So if you go on our website and you try out the tools, I think you'll quickly realize what sets us apart from most fraud prevention providers is the fact that from a go-to-market perspective you can actually trial out the product on your own. That's truly something that's new and most fraud companies don't allow for that. You can see the pricing model online, you can look at the API documentation, you can even integrate it yourself.

And if you look at it from a technological standpoint then what you'll find is we're very focused on data enrichment, on doubling down on data enrichment. And what we mean by that is there's all these fraud providers out there who've been around for five, 10, 15 years, ever since online fraud has been a thing and they've built their product portfolio based on the fact that they are saying that hey, we've seen ten years worth of fraud. We know if an IP address or an email address has been involved in a fraudulent transaction five years ago, so that IP address should be fraudulent today as well and we'll tell you that because we have the biggest blacklist that we've built up in the world. And so, what we've done is at day one we don't have a blacklist of data points so we said, what is it that we can find out about a specific email address online.

You know, let's take peter@gmail.com, I'm sure you'll have some, you know, Facebook profile or an Instagram profile or at least a LinkedIn profile related to your email address and there's means to actually find that out, that's all publicly available information, whether you have that email address registered on these various social media platforms or whether your email address has been involved in any data breaches. And that's just our email module broken down to a very simplified explanation of what it does, but we do very similar things based on phone numbers, based on IP addresses, device information and so on.

And then lastly, if you think about that, on the one hand we have these modular features that you can use on your own and I think more and more companies are moving towards adapting or wanting to adapt these modular pick & mix features that they like and they can build it into their own stack of fraud prevention tools. Or, on the other hand, we offer this as a packaged product, that does end-to-end fraud protection. So, I gave you a very long answer, I'm sorry about that.

Peter: No, that's good.

Bence: Tackle it from multiple perspectives.

Peter: Yeah, yeah, so that's really helpful. You talked about data enrichment and you're really trying to find as much information about, like say a phone number or an email address, you are just using publicly available information, that you're not sort of got any proprietary databases or anything?

Bence: Correct, it's all publicly available. And the reason why, I would emphasize why that's important is, you know, you may question consumer privacy becoming and privacy awareness becoming a hot topic in recent years. You may question hey, you know, I put in an email address in your system and then all of a sudden, I can see all this information about my email address and you're questioning, is that really legal, is that fine for us to be looking at that information? And the answer is, yes, because all we're looking at, we're not looking at how many friends do you have on Facebook because that's private information, that would be breaching terms of service. But seeing whether an email address is registered on Facebook or not is actually public information and we only collect public information.

Peter: Right. I tried out your tool before this interview because it's there on your Home Page where you can just type in an email address and I typed in one of my old email addresses. It's still associated with my LinkedIn and my Twitter and, you know, I can see that you've got some information on me and anyone can just go on and just actually type in an email address and find out what's out there, I guess. So, question though on all that is the fraudsters are also getting better and it seems like you're very transparent which is great, but obviously the fraudsters are going to be on your website trying to kind of reverse engineer everything, I mean, how do you kind of approach that?

Bence: That's a very good question because....so I recall when I was writing in 2017, when we started working on this as a full time project and after raising some early funds, I was actually writing our earliest blog posts and our view with my Co-Founder, Tamas, was always to be thought leaders in the industry. As much as I don't like that phrase in itself, we did want to want to convey information that would be useful for fraud managers, fraud and risk managers.

But then the question is, the more information you give away to fraud and risk managers around, you know, the way fraudsters are doing fraudulent activities and what they knew as fraud trends are and so on. How do you balance that with like, exactly what you said, where fraudsters are researching topics or let's say somebody is a wanna-be fraudster and they're just reading up on hey, how do I become a fraudster and they read one of our articles and blog posts and they're just going to become smarter from that information. And funnily enough, we actually had a case where one family found one of our articles that was focused on fraud trends in a dark web forum for fraudsters so that was really like wow, they do feel like they're threatened by us and the information that we are conveying so that was interesting to see.

But I think that's a fine line to balance and relatively hard to balance when your ethos is to democratize what you're offering, right, like you know, make it as easily accessible to as many people out there in the simplest form possible because that's what's going to make an impact and drive companies to easily adapt your fraud tools and enable them to actually stop bad behavior, bad consumer behavior. That's been an ongoing debate internally for a very long time, but, so far, we've adapted to almost be that, not an open source exactly, but going the direction of making as many things available without a barrier because we believe that's the right way to go about it.

Peter: Right, right. So then, what about like the fraudsters now are getting more sophisticated and they'll create an email address, they'll create multiple social media profiles to make it look a real address. Sometimes they'll spend a couple of years before they do anything to pounce with that identity, when can you tell or how do tell that a synthetic identity has been created purely for fraud versus someone who's just getting online for the first time and they are an upstanding citizen?

Bence: Good news is fraudsters are generally lazy people (Peter laughs) and there's also like the more effort they have to put in, the more they are eating into their own margins of doing business, right. So, if they have to, let's say they have to create email addresses and then park them for years before they can actually start doing fraudulent activity for them, there's the risk that by a year later, like say 12 months out, by the time they would start utilizing that email address, fraud trends have changed and fraud prevention tools have evolved and the loophole is no longer going to work. So, fraudsters, they generally go for short term gain over long term gains, that's like a fact and they try to do things by the mass, as in they'll set up a hundred email addresses a day, they'll try to create a hundred fake accounts out of that and register it and if something doesn't work it's like 30 of these accounts fall out then they'll have 70 remaining.

So the point I'm making is they start with the mass and then they try to like figure out what works, what doesn't work and then in the end they'll have five working accounts out of a hundred and they've successfully, you know, I don't know made a thousand bucks during that day and they're happy and they do that tomorrow and the day after and the day after. So, what I would say is that makes our job easy because if they take that stance and that's the way they work and that's what works for them then our job is easy because that means that you can differentiate, based on some of these patterns you can differentiate what a real consumer looks like and what a fake one looks like, just one that would like to seem real.

And so, that's why I would say yes, fraudsters are one step ahead, but sort of patching the loopholes always makes their life hard and they don't play the long game, they usually play the short game and hopefully, you know, I do believe in a world one day when we can fix everything and we will have an ideal way of living without any dishonest activities at all. (Peter laughs)

Peter: That would be a great thing, but it may be a little idealistic. You mentioned it before, like a fraud-free world, would that mean that no one's trying fraud or that all fraud is being caught?

Bence: Well, I'd say all fraud is being caught because if no one's trying fraud then I'm going to go out of business. (both laugh)

Peter: Well, I don't think you have to worry, seriously, I don't think the fraudsters are going to stop, right. Well anyway, let's move on, I want to touch on account takeover fraud. This is something that I've been reading about a bit lately, can you explain what it is, how it happens and, you know, what companies can do to protect themselves.

Bence: I'll give you a simple example.

Peter: Okay,

Bence: Actually, I recently had a friend, it was very sophisticated. I had a friend who was the victim of account takeover. This is like so close to me because he explained it to me and we know another person that got scammed by it just recently. So, in Hungary there's actually people calling up everyday people on the phone so the caller is impersonating themself to be a bank, a worker of a bank and the number checks out. So, the number is the bank's number, there's an emulator which they use, it's voice over IP, you can easily do that, like you or I we could be using anybody's number to call another person. They call up and they say there's some interesting transactions going out of your account so we have to get into your accounts and we have to take your money there and transfer it to like a safety account where until we investigate these interesting transactions we're just going to keep that money there, like safely.

And then people fall for it, you know, they go on, they talk a couple of minutes about like what these transactions look like and psychologically you're like oh God is this really happening to me and then they try to get into your online bank accounts. Sometimes, my friend actually, he was not smart enough and he submitted his…..he got a two-step verification SMS and he submitted the code to this person while they were talking on the phone, the person logged into their bank account so that's account takeover right there. Now, they're in your account and they started transferring the funds, he had all his money in dollars and in Hungary we use forints so they started converting the money to forints so that they could wire it out altogether. And when they were trying to wire out, it was about $20,000 worth of cash, they were trying to wire it out and that's when the bank system caught that something's going on, you know, like something's not right.

Probably, I guess, if I'm thinking from an architectural perspective of a fraud stack, it was probably a combination of like unusual log in activity from an unusual IP address and a device that you would not normally use, meanwhile, you're doing multiple conversions from one currency to another and then you're trying to send all of that money out in bulk to an account which you've never sent money to. If I'm thinking like fraud rules that's what would happen in the background and that's probably how their system caught it. So, luckily, he was not the victim of this, but I know other people that have been the victim of businesses like a Hungarian, like recently.

This has been a fraud issue happening in Hungary, that's a classic case of account takeover, but they can do it via phishing emails and whatever, you know, they may seem, like they send you an email, it seems like it's your PayPal account or you're due to pay your, I don't know, your bills and then in reality it's not even that company that would be sending that email and it's just a phishing scam and you submit your details and they steal your account basically, yeah.

Peter: Got it, okay. Who are you working with, can you give us some of the names and the types of companies that are using SEON.

Bence: One that I'm really proud of and probably many people know is Revolut, I'm very proud of winning that name over. We are working with Nubank from the Latin American region who I'm very proud of, again, working with Patreon from the US, just to name a non-fintech player as well. Yeah, so a couple of big names from our portfolio that I'm really proud to have won over, especially seeing that I was early on I was actually doing the bulk of the sales, I was running our revenue operations up until the one million annual recurring revenue. Then Jimmy Fong, our Chief Commercial Officer came in

and took cover and he's doing a much better job at it than I ever was, but, yeah, there's a couple of big names and I'm very proud of them.

Peter: Do you also work with banks or is it primarily, you know, non-banks?

Bence: Neobanks, I should say, so Nubank and Revolut, they're both great examples of like the new wave of banking, I would say.

Peter: Okay. So then, can you explain the business model, is it a SaaS-based model, is it the number of API calls, how do you kind of make money?

Bence: Sure. It's purely usage-based. So, let's say you're a company and you have 10,000 registrations a month that you'd like us to monitor or 10,000 transactions a month that you'd like us to monitor, it doesn't really make a difference. It has to be an online point of authentication, right, so somewhere where we can actually see a phone number or an email address or a device or an IP. And at that point, you integrate our API, we start monitoring those transactions or registrations or log ins and at the end of the month, based on your usage, we would send you a bill with the given volume and the given unit cost, the higher the volume, the lower the unit cost goes.

That's purely usage-based, end of the month, we don't lock you into any yearly contract or anything to that extent, there's 30 days notice so it's much like a Netflix account from a business model perspective as in you can step in or step out anytime. If you want to integrate it, you can integrate it in the middle of the night without any sales touch point, but if you want to talk to our sales team, we're more than happy to, you know, lead you through our demos and give you education around how to use the system and what it's best for.

Peter: Right. So, that's how you're able to give it away for free, like there's a maximum usage that you give away for free, right?

Bence: Correct.

Peter: Okay, okay, that makes sense. So then, I'd like to get your sense of the battle that we're having. We touched on this earlier, but I just want to get a sense from you, like obviously there's still fraud happening, you said the fraudsters are lazy which is good, but it seems like it ebbs and flows. We all know about data breaches and how much information is out there on the dark web, but where would you say we're at today when it comes to the fight with fraudsters?

Bence: Hah, that's a great question. The reason why I think about it is because now that you asked me that, I was trying to think like where were we back when we started like let's say 2016, 2017, 2018, like have I seen anything change. And I think the major thing that I've seen evolve is the way that fraudsters are operating as in like techniques that they adapt because like I said before, they always have to find new loopholes that are being patched up. So, that's one way that something that worked five years ago is probably not going to work today, and that's kind of stating the obvious because five years ago no companies had adopted phone number analysis to the extent where they are adopting it today because obviously we're providing such a tool and there's not many other providers out there.

What I am excited about is, like one thing I want to say is I don't believe in us being the ultimate tool that's going to solve your problems in the world when it comes to fraud prevention. What I do think, if you're a successful business and you're dealing with fraud, the way you should be thinking about it is, like there's many solutions out there, how do I apply a multi-stack approach and how do I holistically take a look at my user experience, my onboarding journey, and where do I fit the right fraud prevention tools in there. So, let's say, you know, use something frictionless like our solution at the point of registration and then at the point of transaction or, I don't know, putting in money if you're a wallet, let's say you're a crypto wallet or you're Revolut, at the point of uploading money into the accounts then, you know, have ID verification or at the point of withdrawal have ID verification.

It also depends on the regulatory side of things as well and in the meantime, apply something like, you know, two-factor authentication and you can throw things in there to spice it up. But the point I am trying to make is as I think about fraud and fraud prevention today, you have the most available technology than ever before so you should make use of it as a company. And if we're looking at the fraudster side of things, they are lazy, but they are getting smarter, I think it's easier than ever for them to share information with one another because with crypto currencies we're enabling them to exchange goods and services anonymously. With the world of Tor and Telegram and VPN and Proxy, we're enabling them to pretty much stay anonymous behind that screen so I think fraudsters are definitely in a good place, but fraud prevention providers are also evolving and businesses are in a good place as well.

Peter: Okay. So then, that just brings up another point. It seems like your tools are all in the background, they're all invisible to the user so there's no friction at all in using your tools. So, when someone types in they might be opening up a new account, they'll type in a whole bunch of information and then they'll hit enter and in that moment you're going off doing your tools. And then, are you just giving back a score, are you giving back yes, this is a likely fraudster, what are you providing for the user, for the customer that will help them know that they should take more action here?

Bence: Yeah, you're absolutely correct in the fact that the customer doesn't feel that they're being monitored, it's invisible. You know, they would be submitting that information anyway, it's not like you're uploading an ID where you actually have to take a selfie and a picture of your ID and then you've got to wait a minute until it's approved, that doesn't happen. Our system runs down in a second or less and then the question is, how does the company consume that information, how does the business know whether I should approve somebody based on that or not and there's ….I point to that space, but there's two major ways of using our tool, either you just rely on these modular APIs where you want to make better decisions or you need to use the data based on the email address or a phone number and you just want to look at the raw data, as in like, is this email address registered on Facebook, LinkedIn, true or false and many other social platforms and then, I, as a business, I'll decide what I do based on that raw data.

The other extreme is we have the complete end-to-end solution and we give you a fraud score and you can even trigger these rules in our system and we will actually get you an approved review or decline state once the transactions run through our system. That really depends on the use case and the company and the way they want to use it. The bigger the business, the more they just rely on raw

data and they want to handle everything on their own end. And I'd say SMBs, they would focus on just adopting the whole tool advancement too and relying on our fraud module in itself.

Peter: Right, got it, okay. Are fraud attempts increasing? I'm thinking about the economic cycle and the fact that we're not in a recession yet, at least here in the US, but does fraud follow economic cycles, is there more fraud when times are tough?

Bence: Yeah. There definitely is because it's easier to trick people, right. So, let's say you just lost your job, maybe you're applying for some social welfare, you get an email about it, you submit your social security number there, you upload your ID and you realize it's fake, somebody just stole your information. Or, let's say you see a job application coming your way and then you actually go through the interview process and then they…we've heard of cases where they use that specific video, you know, at the end of the video they would say like oh, please, now we've got to verify it's really you so hold out your ID next to you, turn your head left and right.

And then they would use that video to open a bank account in your name with a digital bank, for example, and then they would use that for money laundering and so on. Really crazy how to the extent that fraudsters take this and really the things they've come up over the years, but, yeah, I definitely think that when there's economic hardship, when there's cycles of a downturn, we are going to see more people vulnerable, more people being the victims of fraud.

Peter: Right, right, okay. So then, last question. What's on tap for SEON in 2023?

Bence: 2023, from this point on, I should say, we're focusing on diversifying our product portfolio and data enrichment. We've been very strongly focused on building out our core products based on this and so we're just going to add additional features, one of them being that we're going to be launching soon is focused on anti-money laundering and sort of screening the PEPs and sanctions lists, so that's one aspect of the business that we're strongly focusing on right now. Taking a look at the current global climate, there is a higher and higher need from businesses to be able to screen this.

What we're doing, based on data consumer analysis today, we think that can easily be applied for actually analyzing businesses opening up online accounts as well so we're going to be developing a product focused on that later down the line. I don't want to spill any more beans around it, that's truly a secret sauce. Our key focus for this year and the coming years is releasing more products with the focus on what we've been doing, so far, which has worked really well for us. We've scaled really quickly, we've won great businesses over so now we're focusing on diversifying our product portfolio and releasing more products around what we're doing already.

Peter: Okay. We'll have to leave it there, Bence, thank you very much for coming on the show. You're doing good work here and it's important work as we always try to stay one step ahead of the fraudsters so thanks again.

Bence: Well, thanks for having me, it was great talking to you.

Peter: You know, it struck me in talking to Bence there that while the tools are essential for fintechs, banks, anyone in the financial space to have the most robust set of anti-fraud tools that money can

buy, I feel like that's essential, but it's the only piece of the puzzle as Bence shared there, like people are getting phone calls from companies they know, they're getting emails obviously all the time.

It just reminded me that as a consumer, we have to be vigilant, we have to make sure that we're not falling to scams. Anytime someone's asking for personal information, anytime, whether it it's a phone call or email or what have you, you just have to be 100% certain, you have to be extremely careful. That's, I think, the only way that we're really going to ever beat the fraudsters is if everyone is a bit more vigilant and obviously tools like SEON are going to get better and better as well.

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

(music)