FINTECH ONE-ON-ONE PODCAST NO. 408-KEVIN GOSSCHALK

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 boutique all meetings event, Dealmakers East, happening at the Ritz Carlton South Beach on February 7th and 8th. Dealmakers East is all about meetings, there are no keynotes, no panels, it is 100% focused on hand-curated meetings, whether you are looking to meet fintech CEOs, bankers or investors we have you covered. Our Dealmakers events have consistently been our highest rated events so go to fintechnexus.com to find out more and register.

Peter Renton: Today on the show, we are talking about fighting fraud. I'm delighted to welcome the CEO & Founder of Arkose Labs, Kevin Gosschalk, to the show and we are going to talk about the different ways that fraudsters are operating today, how they are evolving, how they're getting smarter and this new concept of like Cybercrime-as-a-Service and how that has changed the game and what it means for fintechs. And so, we talk about the different types of fraud that we're seeing, how the fintechs should be addressing it and we talk about some of the ways that Arkose Labs is able to combat some of the fraudsters. We talk about the friction between a good user experience and solid anti-fraud measures, we also talk about what it's going to look like in the future, where the next wave of attacks may be coming from. It was a fascinating discussion; hope you enjoy the show.

Welcome to the podcast, Kevin!

Kevin Gosschalk: Thanks, Peter, good to be on.

Peter: Great to have you on. So, let's start with giving the listeners a little bit of background about yourself, I know, like me, you are from the land Down Under so why don't you tell us a little bit of a background and what brought you initially to this country.

Kevin: So, I'm kind of an engineer by trade, pretty strong gamer as well, that's kind of where I started my life playing video games and loving technology. I actually studied at Queensland University of Technology in Brisbane, Australia, studied Bachelor of Games and Interactive Media kind of a very left field considering that now I'm running a security company, but, yeah, there's a few things I did that were very different from games, I would say.

So, the first thing I did out of University was I helped a research study looking for early markers in diabetes, of all things, so I actually helped build technology which would let them map nerves in the

eye and it turns out at 500 times magnification which is quite a large magnification, I would say. The nerves actually are really good indications of whether a patient has diabetes or not. So, if you have a healthy nerve system, you don't have diabetes, the nerves all kind of whirl together, like it's very distinct, it's very obvious, you can see it clean and clear as day. For someone that has diabetes, they were broken up, they actually don't converge as a whirl. So, just looking at the eye can actually tell the difference between someone with diabetes or without it and that technique works two years earlier than traditional blood pricks and other techniques that they use.

So, that study was looking for early markers for diabetes and they were trying to figure out, how do we build software or some way to map this because the problem with putting a camera on someone's eye, you need to kind of take photos of like a very large portion of the eye before you can build a map. And people were very twitchy with their eyes and if someone twitches their eye at 500 times magnification somewhere else in the universe basically. So, I kind of built a technique using kind of game technology and interactive software that let us map the eyes and then I wrote software that let them automatically stitch the photography together so we used some computer vision and machine learning software that did that. So, I did that for about two years, so I built the pioneering technique that they did a then seven-year clinical trial on and they now actually use that software in the UK to help diagnose folks. That was kind of a small contribution to health.

After that and actually in sequence to that, I was working on a scholarship project with the Endeavour Foundation which is a large not-for-profit in Australia for people with intellectual disabilities. They wanted to kind of get something that got people up and active. So, again, kind of back to my gamers-roots and kind of pairing that with interactive media so like tangible media, like stuff like levers and cogs, and stuff you can pull that makes something happen. I kind of built this prototype system, got a $5,000 scholarship which gave me some money to buy some stuff from a hardware store and the electronic store and stuff that kind of jury-rig something together. We built this kind of 2 x 3 meter interactive floor so it was like a giant iPad on the ground.

The way that I made it actually work is I got a bunch of sensors you put under your mat so when you step on the mat it would trigger the house alarm, this was back before cameras and stuff were a thing and got 60 of those, wired them in array and wherever you would step, it would basically act like a giant button so I would know you are stepping in this giant 2 x 3 meters surface and I would put a projector on to that and then I can project like a game kind of experience like you walk through a puddle, a pool or a giant keyboard. We commercialized this with the help of the Australian government actually as a research commercialization grant, they've re-named it a few times, depending on which government is in power, it's Accelerating Commercialization or Commercializing Australia or something, I don't know, they kept re-branding it.

But it effectively funds innovative research in the new kind of technologies, and we ended up commercializing this, we worked in partnership with Microsoft and we were the first third party using PC technology for the Microsoft Connect which is like a depth sensor to determine how far or how close you were from an object. So, I have a bunch of experience like computer vision research and stuff like that and that ultimately, we licensed one of the largest education providers in APAC and they actually now still have that technology that they, you know, we ended up kind of pivoting a little bit into that early education because it was really engaging technology and can do like learning activities and stuff with it.

So, I have a lot of experience in what machine are good at recognizing and understanding and then kind of turn that to the reverse field which is security web. We're now trying to stop bots from getting into services and websites and creating accounts and compromising accounts and took the knowledge from building that kind of software to then understanding how to feed that kind of software and so preventing those feeds from understanding and how recognize and get through things. That's kind of what is the pioneering idea behind Arkose which we've been incredibly successful and remain so today with our kind of approach there. You know, the key objective of the Arkose product is to basically make the cost to adversaries higher than their profits, turns out if you do that, they stop, so that's a pretty simple concept, right?

Yeah, that's kind of the approach that we take to the kind of product we build and, you know, as an Aussie, who really better to run a security company, we're all convicts by birth? (both laugh) Who better to explain the criminal mind, right? I moved to the US about five years ago and that was really because all the companies we were working with, you know, some of our early customers were companies like GitHub and Dropbox, you know, Roblox was an early customer, all very large US businesses with global products and they are the most lucrative for attackers. They really want to go after large, user-bases and things like that so, you know, we're a really a good partner, a good fit for those companies. I was on a plane every month.....

Peter: Oh, my God.

Kevin: .....moving back and forth between Australia and the US. At a certain point, it was pretty obvious I had to not do that anymore.

Peter: (laughs) Right. Yes indeed, okay. So then, let's just maybe, give us a state of play dealing with fraudsters. I mean, what are the biggest challenges today when it comes to fraud attacks, particularly looking at it through a fintech lens.

Kevin: So, we saw a really big shift in the dynamics, I'd say over the last 12 months, that now just really favor criminals, unfortunately. I think it's getting worse and I think it's going to be really tough in the coming years. So, the use cases that an operation protects and kind of our perspective, so we work with some of the largest fintechs in the world, obviously the largest ones in the US, we work with a lot of non-fintechs as well, the video game merchants, we work with the big tech companies like Microsoft, we work with big travel platforms, the big retailers, so we really kind of see it all.

For a fintech, you know, the target, of course, is money because that's what fintechs have, there's really two areas that we protect that would be relevant, creating new accounts so it's something that's abusing your new account experience, opening cards, taking advantage of promotions where you're funding, maybe a few dollars into a new account, whatever it may be so that's obviously one big area. Then the other big one is account takeover so that's one of the areas, account takeover kind of has two flavors of attacks, one is credential stuffing where they're reusing usernames and passwords because that's, unfortunately, what you probably do, and all of the listeners unfortunately probably do...ideally shouldn't do that. The other component is social engineering so that's where fraudsters talk or send something, get someone to click a link, whatever it may be, and compromise the account that way.

In the context of fintech, compromised accounts can turn into money, right, so they want to compromise an account that has funds in it, or can turn into things like micro deposit fraud where they're funding accounts or creating accounts where the objective is to basically get people to deposit a few cents into their real bank account to verify you own that bank account, you know, depositing a few cents and they do that hundreds of thousands of times and they make like a few thousand dollars a day from doing these kinds of attacks.

So, there are different kinds of attack techniques and again, of course, it's all for-profit so the adversaries are trying to figure out, how do I scale these attacks, how do I make these attacks in a way that's cheaper than my cost. Credit cards, for example, you know, you can completely bypass KYC by just buying a valid identity, you will pass KYC if you have a valid identity, you know, anywhere from $7 to $17 you can completely bypass KYC. Well, not bypass it, you're passing it correctly, you've got a valid ID like it's actually, you know, KYC's job is to validate if the ID is legit, it is legit, unfortunately, that works, but they might be able to make $500 from passing a KYC process so the barrier to entry to prevent these kinds of criminals has to be quite high. And the thing that's really the favorite of criminals is node sharing so there's a lot of communities like Telegram, Discord, etc. where criminals share knowledge on how to make these attacks, who are weak targets, what are good techniques, I'm being blocked by this, what should I do? And they're more than happy to share that kind of information.

The other problem is a huge rise of what is called Cybercrime-as-a-Service so these are kind of kits that are ready to use, that can bypass defenses, that can do proxy site cloning, they basically do everything for the fraudster, the fraudster himself doesn't have to do much other than say, here's my victim I'm going after, here's my bank account, go fill it up, I'll buy the software and there's developers that basically build that software. And this is a huge issue because the cost dynamic is quite different when a bunch of people are pooling their money for one development source, versus a fraudster attacking and trying to figure out by himself. It's really shifted the balance dramatically, I think, in the favor of the adversary.

Peter: Who's the buyer of this like, you know, Hacking-as-a-Service, are these just, because I imagine the big time operations have their own, but these? Is there someone looking to become a criminal or they're already a criminal and they're looking to expand their business, I mean, who buys it?

Kevin: Yeah. These kind of services are just demonstratively better than any of these others that have come before them, even the big riggers are now using the services versus maintaining their own software.

Peter: Interesting.

Kevin: It's kind of like how SaaS impacted the real world, it's kind of the same in the cybercrime world, it's like hey, I'm building a stuff in-house and my cost is this, my effectiveness is this. If I outsource it, my cost goes down, the effectiveness goes up, why wouldn't I do that? That's kind of what we're starting to see to the point where, you know, we used to see dedicated adversaries on a customer-by-customer basis. Two years ago, three years ago, four years ago, that was kind of what it was whereas now, we primarily have to beat the Cybercrime-as-a-Service platforms.

Peter: So, that's why you said it's getting worse, right, where the fact that these Cybercrime-as-a-Service are more effective, overall.

Kevin: They're more effective and the communities are bigger and the communities are good at sharing how to use the services, that's kind of the glue that kind of holds it together as well. There's just an incredible amount of knowledge sharing on the fraudsters' side which, unfortunately, we don't really do in our industry and that is a huge disadvantage to people trying to prevent criminals.

Peter: Okay. So then, the question obviously, you've teed it up, but how do you stop this Cybercrime-as-a-Service?

Kevin: Yeah. I mean, that question is what everyone's trying to figure out, right, because I think if you're trying to build defenses in-house, you're going to get really quickly behind how quickly they adapt, like they adapt within hours, like they can re-build defense attack tools in hours, that's how quick they are, they're very entrepreneurial, they're happy to work many hours, many days. We do see them take weekends off, it's actually really kind of funny on Christmas we saw a huge number of attacks, you know, one customer they were trying to prey, like 70 million accounts is what they were attempting to create, these are big numbers, right?

Peter: Wow!

Kevin: Just this weekend, they stopped attacking for like two days and this is a massive plummet in attempts, it's kind of interesting to kind of see that because the attacks are not successful, but they're continually trying different things and we keep seeing like…because we use their services, we kind of buy from them, right, like we buy these services to see their effectiveness and we use those to figure out like how to mitigate it and stuff like that, it's actually kind of fascinating, our research efforts on this sort of stuff. So, we're always kind of monitoring to see, how're they complaining that their approach against Arkose, is it working or not working. We're not seeing a lot of that from the other companies and sites they go against so I can only imagine the effectiveness is really quite high as a standard.

So, I think it's really going to go back to basics which is you've got to build something that inherently is more expensive to attack than it is for a fraudster to profit from. That can be a bunch of things, it's not just using an Arkose, you can build the product in a way that is naturally difficult for a fraudster to make money, withhold refunds if you're like e-commerce. In the context of like fintech, withhold approvals in certain scenarios until you kind of vet it out further because all of that decreases their motivation and their profit margins so that's really kind of the name of the game, it's like how do you build something that inherently as a product isn't good for a fraudster. Unfortunately, due to the nature of how fintech likes to grow, everyone likes to grow really quickly, they're incentivized to give away quite a lot of money for like promo credits, you know start up and get "x" dollars, that is just like, as you can imagine, quite attractive to criminals to go after.

Peter: Putting these roadblocks in place for the criminals also can lead to a poor user experience so you can add friction and have very low fraud or you can have no friction and higher fraud, how do you balance that? What are some of the things that you see and best practices with fintechs?

Kevin: That's a true statement! If you turn off the sign up, you'll have no fraud, it's great! (Peter laughs) You also get no customer complaints, that's another good benefit. You get some revenue problems typically on that one, but it's got to all be risk-based, you've got to do everything on a risk-based model, that's kind of been our approach since the beginning. It's low risk, you just let it on in, like if it looks good, seems good, you know, you probably should take the chance because otherwise you're not going to have that much of a business, right, but then it's got to kind of scale up and your defenses have to scale up too.

The more, sure that it's a bad thing like, for example, you might typically see a ton of fraud from like one region in the world, maybe like the US you see low fraud, but maybe from Vietnam you're seeing a high degree of fraud coming in so you can just simply have different rule sets for those two regions, right, like maybe in the US you're a little bit more lenient whereas in Vietnam the moment that you see anything that's a bit strange, you bump it up to like the next gear, right. Or, if you see like the high volume of really bad stuff, in an already well-known risky region, you put that on like super high, like maybe a manual review of kind of level of friction, right.

Peter: Wouldn't they be using VPNs to like mask their location?

Kevin: They do. There's ways to kind of detect that sort of stuff so, for example, time zone matching is something we found very interesting so typically the VPN, and the time zone of the geo coordinates, the IP address is different from the time zone of the device that's using it.

Peter: Right.

Kevin: Those things can be masked. I think with sophisticated, like automated attacks and stuff like that, that's typically masked, but with kind of the lower volume manual fraud where it's just like a person is doing it, you'll be able to catch some of those kinds of things because they're not typically that sophisticated. If they're using like their own phone, they can't really easily change the time zone and, you know, so it does differ depending on the type of fraud, but you are correct. I mean, ultimately any data sent to you from the customer can be spoofed if they want to.

Peter: Okay. So, I want to just talk about credential stuffing which is sort of a relatively new term to me and the fact that, you know, you have this...I think you have a guarantee on your website.

Kevin: A warranty.

Peter: Yeah, yeah. A warranty about a million dollars credential stuffing warranty, so tell us, what is credential stuffing and what is your warranty and how are you able to provide it?

Kevin: Yeah. So, credential stuffing is.....due to the fact people re-use passwords on multiple products, apps, websites, this isn't a secret. We know people do it, the data's out there, it's very unfortunate, but it is kind of what it is. Once one website gets compromised, which as we all know is happening pretty frequently, there's been more than 11 billion usernames and passwords that have been leaked through compromises, so it's just this ridiculous number of combinations that are quite well known, what attackers do is they take those previously leaked usernames and passwords and

then they go to any high value login page where they want to get into accounts because there's something of value.

Fintechs obviously have quite a lot of value in the accounts, they use automated software so they use a bot, there's tools that do this, there's a tool called Openwall, it's an open-source piece of software and will automatically do these attacks for you. You just put some names and passwords and it will make the attacks, but it basically tests the combination so it's looking for valid combinations so it's just continuously putting in those usernames and passwords and it's stuffing the credentials into the login page, so to speak. You don't want that because eventually they'll find combinations that are valid and they'll get into the account so there's a number of strategies to mitigate that.

Multi-factor is a big common one in the fintech industry so the reason why you have to do multi-factor is because of credential stuffing, otherwise, you wouldn't have to do multi-factor that made that kind of a really important requirement just because it's so easy to kind of break usernames and passwords nowadays. Not all fintechs mandate it because it is really high friction, multi-factor is a lot of effort to enable, it's a lot of effort to do every time you login. And it also is more designed for preventing social engineering and there's better defenses to stop credential stuffing that are less friction, obviously Arkose Lab is one, but there's a number of others out there as well. That kind of the sum of credential stuffing.

In terms of the warranty and why we offer that, so in our space, you know, stopping attacks on, you know, log-ins, and sign-ups and things like that, really when you work with a vendor it's a best effort, you don't really know if it's going to be able to stop the attack, you don't really know how long it will work for, like an attacker might build a tool kit that makes your vendors not work after six months, like it will just bypass the vendor. You just have to be really good at looking human enough so that it basically says they could let them in. So, that is an arms race that, unfortunately, does have that kind of consequence if you don't have the right tools, that they're actually are going to get past it entirely.

We have the conviction and confidence, our approach, tools, technology, and our security operations center team who review things are able to prevent any attack like this - period. And we've been able to uphold that for many years. Basically, what we decided was to stand apart in an industry where no one was going to back or certify their product would work, we're going to come to market with a warranty. That warranty effectively states that if the Arkose product at any point in time can't prevent these kinds of attacks, not only will we cover up to a million dollars in losses if anything gets past us, but it actually is an opportunity for the customer to reassess do we want to keep working with Arkose?

There's no other vendor in this industry that will have a clause like that in their contract, they just don't exist, and we've had this warranty in our market for almost a year and no one has come to the table with anything even close to it within our space and that should really make companies think about who they're choosing as partners. I think pick a partner that is in it with you to win or pick someone that's best efforts because that's really kind of the table stakes right now in the space we're in. I'm actually kind of disappointed we're not seeing anyone else launch something like this in our space.

Peter: Okay. Well, I want to talk about CAPTCHA, that's been around for a long time and I get annoyed when I have to match the traffic lights or the bridge or whatever it is and it's kind of annoying

and you've come up with a better system. Tell us about Arkose MatchKey and why it is better than CAPTCHA?

Kevin: Yeah. Let me first describe CAPTCHA. So, CAPTCHA is a Completely Automated Public Turing test to tell Computers and Humans Apart, that's what that stands for. So, the intent of it is let's say automated test so a bot creates the test and the test is meant to be able to validate are you a human or a bot? So it's a machine validating your authenticity. It's a kind of strange concept, but that's effectively the intent of what a CAPTCHA is meant to be.

Now, the effectiveness of the CAPTCHA itself depends on a number of variables, how well is a machine at doing activities that it's being asked to do, things like labeling photos. Just AI has gotten so good at that now that that really doesn't work as a way to test if it's a machine or a human anymore because machines are actually better at labeling data than people are in most cases as long as they have a large enough inventory of examples to work from which obviously at this point in time on the Internet, they absolutely do. So, these kinds of tools like select the street sign, like that technology is kind of quite dated, like it's six/seven years old now. If that's your core defense, that doesn't really work anymore. If an attacker wants to get through there's plenty of ways to automate past that, machines will figure that out over the years.

Really, to be effectiveness in the game of testing for automation with a test, you have to build something that inherently machines are not good at doing and there's no value in them getting good doing it because if there is, obviously, eventually AI catches up and the tool won't work anymore. So, the strategy that we deploy from a challenge standpoint is just that, let's build something that inherently is only designed as a security test and is simply designed to be, at that point in time, better than what commercial software can recognize from a computer vision standpoint which is kind of a technical and complex problem, but kind of important to building good software in this space. And the challenge, we will use it only on risky traffic or clearly abusive traffic, you don't want to use friction like that on good users, obviously, as you said, annoying and cumbersome, all those kinds of things.

The alternative though is if you don't have someone like CAPTCHA is blocking the traffic so you tell me what's worse, being blocked entirely from signing up or solving a small puzzle. That's kind of where we're at right now from defensibility against automation, it hasn't really changed, but the puzzles themselves have gotten worse over time because machines have just gotten better. You see things like chatGPT like AI is doing fantastic things now, like you just can't rely on these older defenses anymore so we kind of built this new one. What it does is it uses two 3D models and we generate a question and then we generate a visual puzzle dynamically and the objective, again, is to build something that's really expensive for adversaries to write software that can recognize how to get through it.

This new MatchKey technology, you're matching a key image, very creative naming, is really probably the best that we've ever designed and by far better than anything that we've seen before in the CAPTCHA history on the Internet, so far, to date in that it really excels in the usability side, so it's taken our knowledge over the last seven years of building defense in the space around what kind of problems are really actually expensive and difficult for adversaries versus not what's difficult for AI because that question's changed almost on a monthly basis in the last 12 months or so, right, and use that knowledge to build this new technology.

It really is a re-set for adversaries targeting Arkose because it's just this complete game changing approach on they have to think about how to attack us which they've not have to deal with. It's basically kind of like a brand-new category shift in this space with a company that's been doing this for seven years which is quite unusual, it's rare you see incumbents get the kind of experience, we do build something that's such paradigm shift in the security space.

It's a huge advantage for our customers to have that kind of complete refresh, I would say, as a defense, kind of like what it might be if you bring in new tools, it's going to work really well when you first bring it in because no one knows how to deal with it. And that's kind of how you have to think about it in the security space like you have to continually innovate and build new technology like this, otherwise, your platform gets tired and the attackers figure out how to get through it and then, you know, you go back to the best efforts and they're just not really good enough if the attackers kind of know how to get through the stuff.

Peter: Right. So, I imagine though that eventually these Cybercrime-as-a-Service people will figure out a way, they'll roll it out in their next version of their software. So, obviously, you've got to be thinking the next thing, right?

Kevin: It's an arms race, that's correct, and the objective is simply make their businesses not profit worthy. So, you know, when we roll out this kind of defense, because we're in their communities, we're reading what their users say, we're reading their reviews. The reviews become incredibly negative when their service stops functioning and when the reviews become negative they stop using the service and then they move on to a new service and then something that just goes away.

We've seen that time and time again, I can tell you that, we've squashed many criminal enterprises and we have a long list of all the ones we've dealt with and all the ones we've demolished over the years, both from being part of their communities through to just doing our job on a day-to-day basis. Really the goal is simply to get to the point where their product is so unreliable and unusable that the community stops buying from them and then suddenly go to someone else and then, you know, runs in repeat. So, we're in the business of killing criminal businesses that feels like, that's kind of what the team does.

Peter: So then, what's the life cycle for something like MatchKey, are you looking at this like this is going to last a year, two years and what do you think about it?

Kevin: Yeah. The very cool thing about how we built the technology is it's designed to be dynamic. So, it's a platform, it's not just a single challenge so you can do many things with that challenge format so the format is designed to last quite a long time and puzzles that we haven't even thought of yet will fit into that existing format. That's really kind of the big innovation with how we build challenges at Arkose is it's so dynamic and without even needing engineering results is we can change it completely, the question of raising the type of context, everything and that allows us, you know, we have a 3D artists and stuff like that that are building defenses.

It's very strange, it's very weird we're a design company doing security, but it really lets us kind of innovate quite quickly building new defenses and stuff like that and we don't even know the limits of

that technology just yet because we innovate based on what the attackers do and we learn as the attackers come after us, and that's really kind of the game we play. It's really hard to think about what we should build next until we see what attackers are trying to do so that's really kind of an important part of this.

You couldn't come into this landscape and try and build a solution completely green with no expertise because it wouldn't work very well, like that's kind of the fascinating thing about the space we're in, like the expertise we've built in what we've learned really is what lets us build, think and innovate better than everyone else that's trying to do some of the things.

Peter: Right. So, when you look sort of towards the future then, you know, you said you're in these Discord forums and what have you, they're all sharing information, like how are you preparing for the attacks that are going to happen in 2024, how do you kind of help your clients, you know, prepare for the next wave?

Kevin: Yeah. The strategy we have, which it's consistent, and really is how we do things again is about raising adversarial cost and effort. So, we're building new technology which lets us get additional data points, different signals, things that are really expensive for fraudsters to spoof that let us continue to raise that cost bar, like that's a very important process, that's what really all we can do. All you really can do is ultimately make it not worth their while, if you do that they'll stop and we've seen that numerous times as well, but that is the key purpose from a product roadmap standpoint.

You know, we launched this new MatchKey technology in the last month, we have a new product we're launching early in Q1 around different kinds of reputation sources from data we look at, we launched a new phishing defense last year which lets us look at sites that are set up to proxy your site so bypass multi-factor and all this kind of stuff.

So, we're always kind of looking at what is the new techniques adversaries are doing, trying to lower the cost on their side to raise their profit margin, how to do the reverse of that, how do we reset that balance back in the favor of the fintech or the merchant or whoever we might be working with to ultimately make their service more protected? The other component is we work with the customers pretty closely, it's not just "here's tech, good luck…" We have a managed service team that are constantly adapting and reviewing and tuning things as needed, but also providing insights and working with the customer in that.

You know, if you're launching a promo and it just so happens to be so lucrative that you really can't defend it, because they're willing to basically do whatever it takes to get through it, you might want to re-think kind of how the promo's structured and stuff like that too so even some guidance around, you know, those kinds of things we help our customers with because it is not really something people think about when they kind of think about growing a business. They don't really think about what someone's going to do to abuse it and take advantage of them which is plenty of people, unfortunately, out there that are looking to do just that.

Peter: Right, right. Well, we'll have to leave it there, Kevin, really interesting. I mean, this industry you're fighting fraudsters don't think is ever going to go away, there will bad actors in 50 years time

trying to get through the security system so it's great work you're doing. Thanks again for coming on the show.

Kevin: Great, thanks, Peter, for having me.

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)