Aaron Delp (00:00.838)
Hello everyone and welcome back. This is your co -host Aaron. And our topic for today is really interesting. It's all about fraud detection and personas and personal identities. And so we're gonna dig into that. It's an area we've dug into a little bit before, but probably not to the depth that we're going to talk about today. And so for that, we have Rick Zung, co -founder and CEO at persona. Rick, how you doing, man?

Rick (00:28.818)
I'm good. Thank you so much for having me.

Aaron Delp (00:31.104)
Absolutely. So first of all, welcome to the show and give everyone a little bit of background and a quick introduction, please.

Rick (00:37.772)
Yeah, for sure. So I'm Rick. I'm the co -founder and CEO of Persona. Usually I think I always like to introduce myself by way of my past. So prior to all of this, I was an engineer at Square for about, sorry, Block now for just about five -ish years. And it was a lot of my experiences there that both taught me kind of how to...

start a startup, but also really kind of the challenges and importance of identity. Never did I imagine how pertinent it would be in this world of AI, but at that time, I mean, many of the details that we were thinking about back then continue to apply here. know, Prasona now is about five years old, almost six. We've been working on the space of identity verification and personal information infrastructure for, you know,

all this time and we work with all sorts of customers. mean, one of the most unique things about Persona is our ability to kind of adapt and mold to any type of business out there. So anywhere from a TravelX to a Coursera, from Square to OpenAI, we power all of their identity infrastructure to make sure that they're verifying identities in a secure and robust way and hopefully preventing fraud and also managing the personal information in a compliant but more importantly, privacy set up.

forward way.

Aaron Delp (01:59.974)
Sure, that's fantastic. And so I definitely want to dig into Persona and some of the details there. But before we do, you did mention you kind of cut your teeth at that square or now block. What lessons did you really learn there that you brought forward and what experiences really impacted you in creating Persona?

Rick (02:24.472)
I would say, well, the most obvious one is I learned how to be an engineer there. That was really my first job out of college. So I suppose that might be the most important experience. But

outside that, I think there are a lot of values at Square. The one that always resonated tremendously with me was the value of starting small. And I think that's very different from, you

Aaron Delp (02:29.724)
Sure.

Rick (02:48.908)
These days, especially within the startup ecosystem of Valley, sometimes I think like starting small oftentimes implies almost fake until you make it, like building something that's smoke and mirrors, and especially this era of AI, right? Create something smoke and mirrors and then later on you can flesh out all the details. But start small, especially at Square, think meant something very different, which is start with a small product that was done right. In the world of payments, you really can't do such crazy things, especially in such a regulated space.

And rather than trying to build the vision and then smoke and mirror it up, instead, lay the foundation for the smallest feature that a customer want, build that really, really well. So in the early days of Square, that would be the Square Reader. Make sure that works tremendously well and then expand from there. And I think for identity, it's very similar. We could try something in which, again, smoke and mirrors things, but rather build something small, make it work really, really well, and then grow from there. And I think that was one of the most important lessons, especially if you're trying to build something that is sensitive.

has law of regulations, compliance details.

Aaron Delp (03:51.206)
Sure, sure. And it's funny too because, you know, there's always like this shorthand, especially with startups, it's like, what kind of startup are you? And it's like, we're the Uber of whatever, or a lot of times you'll hear the, we're the square of whatever, and you get to literally say like, you're the square of, you know, identity management kind of thing, right? So in this instance, the analogy plays out directly. Let's talk a little bit about...

you know, personal identities and how we kind of got here, right? Like, so of course, like, I feel like just about every day you see something about personal fraud or like, you'll get a letter from, don't know, somebody, your bank, your credit card, your, you know, somebody, your identity got out, right? Like, I feel like identity theft and personal information leaking into the world just happens more and more. But, but, and so how does that relate to

persona in the fact that like you want to build a secure platform around all of this right like how do you take that Idea and then create an entire framework and product

Rick (05:04.992)
So especially on the topic of data breaches, think this is one of most common questions that we get. And this is one of the other learnings I really got from the world of payments, which is the challenge that we face, and especially the sheer volume of data breaches that we see today, I

don't believe the core cause is an inability to secure it. I think there's two fundamental ones. The first of which is far too many targets.

And the second is lack of incentives to really secure it, especially when you have so many targets. so, you know, the analogy I always give is that within the world, if you're talking strictly about what are the most valuable targets in the world to hack, I mean, there's two that come out immediately. Number one, hacking a cloud infrastructure. If you can hack a native less GCP, every other business in the world's built on this at this point, that is the most valuable thing. you could breach number two is a, if you can, hack a payment network or even one of these like payment businesses and adding a stripe, a square, et cetera.

The number of card information, the immediacy of value that you gain from being able to get access to such a platform is tremendous. But we don't really see that too much. And I think one of the major reasons for this is we're seeing a similar evolution right now within the world identity. But if you look way back, credit card leaks were rampant. Like really, if you look 10, 15 years back, were a tremendous number of data breaches there. I even oftentimes tell folks one of the jokes of my...

I tell folks that my dad used to tell me that the dumbest way to lose all your money is to put in your credit card information online. But today, he doesn't think twice about this. He's on Amazon, he's buying things all day, he's retail -theraping away. I think we're in a similar ecosystem for personal information. The challenges that this space faces, and the reason why there's so many data breaches is there's far too many targets. At this point, at the end of the day,

If you have a thousand companies, you just need to find the weakest link. And as long as there's a tremendous treasure trove of personal information out there, there's an opportunity. So I always like to tell folks the security challenge is not intractable. It's just that there are too many targets and the more companies who want to kind of offload this, secure it with a platform that's dedicated towards protecting personal information, the more secure the overall online ecosystem will be. The second question often then becomes how do you secure it? And I think the most important thing here is defense in depth.

Rick (07:15.842)
building a lot of layers. And one layer that think is oftentimes criminally under thought about is people. Like there's no better way. If you look at half these data breaches, oftentimes they're through phishing attacks, they're through some mechanism over escalation of privileges. More so than ever, I think it's important that you consider not only the infrastructural protections, which I think a lot of modern tech companies do a great job around, but also the people protections and making sure who within our organization has access to all the personal information.

How much can they have it? Do you have audit logging? Can you track anomalies? Can you detect, know, can you add many layers of authentication to get access to this privileged information within the system? I think it's really, really important. So for us, it's a huge area focus for us. And our long -term belief is that the best way to limit the number of data breaches, secure personal information, is to have fewer targets. And for the targets that do exist to be incredibly, incredibly robust and have many layers of defense.

Aaron Delp (08:10.596)
That makes sense. It makes perfect sense. Let me ask you, I almost feel like this has become a table stakes question on the podcast, but how has AI impacted this industry? And what I mean by that specifically is, know, I think that with the power of GenAI tools, the idea of multiple targets just goes up dramatically in the fact that you've got a greater velocity, right? Like you can go after more targets.

and create more things faster than you could before. Is that a correct assessment and how do you see, like does AI become a threat to your industry or it can also be helpful as well? What's your thoughts?

Rick (08:55.736)
So I suppose this actually is probably the common answer that you hear, which is it's both. It's 100 % both. So I always like to talk about the threats first. I think it's the more interesting of the two. Again, working in the fraud industry, you oftentimes think about things that way.

The threats, I think, are immense. And in particular, the ability these days for someone to be able to fabricate, create synthetic identities, high quality video fakes, facial tick over, and lowering the barrier to that. So one thing I always like to tell folks, that generative AI is not net new. There are many ways, even like five years ago, there were incredibly high fidelity ways to take over your face, swap your face out for Tom Cruise's or things like that, right? Those that aren't gone viral. The challenge generative AI really presents is that it's lowered the barrier for that. Like the sheer, like now it's just

couple of prompts with the companies models and especially with the sheer velocity that that space is improving is easier than ever to be able to produce incredibly incredibly high quality fakes. In many ways I think it challenges a lot of the notions of how can we use just pure video and image based verification which for much of the online fraud prevention industry has been kind of the state of the art honestly for the last three to five years.

It's challenging that paradigm shift. And I think the biggest one is that now there's no longer this single silver bullet for how do we stop fraud anymore? For a long time, videos, images, like a photo of your government ID, a video of yourself, you know, performing some degree of actions were relatively like robust. That's not to say fraudsters can bypass it. And many fraudsters have been able to bypass it for a long time, but it was relatively difficult today. It's become easier than ever. The solution, I think more so than ever is going to be, there's not going to be a single way, but rather multimodal.

I think it's actually gonna take a lot of cues from what's been happening in the world of cybersecurity, which is after MFA and then after SMS to FA, the rise of SMS hijacking, like that, prompted the industry to build out new technologies and more importantly, add in a lot of passive detection to be able to say this is a high risk one and combining passive approaches in which you say, hey, this looks a little bit more suspicious. I can't say for high confidence you're a bot, but let me ask you to do something else.

Rick (11:06.998)
I think we're going to see a very similar rise from the role of identity. And there's a lot of companies already doing this. I've heard terminology of this from progressive risk profiling, segmentation, risk segmentation, step up verification, but many, many in the industry are already adopting such techniques. And I think more so than ever, it's going to be a hit on image -based verification. It's not going to be the end in the same way that most 2F8A still performed using SMS. However, I do think the complexity of this space is going to rise dramatically because of this new vector of fraud.

Aaron Delp (11:35.845)
Sure.

Rick (11:36.658)
the good news, suppose for the industry, can't say it's good, but I think it's a tailwind for this space is that for both consumers and enterprises, it's going to be more important than ever to do, identity verification to detect AI. And the reason why I say this is that what really AI does for consumers is that it makes it such that content moderation, especially automated content moderation kind of is dead. There's just no way at this point to be able to tech.

that some contents were in by AI. I've seen many approaches out there. I don't think anyone has found a lead. OpenAI published a paper just a couple of weeks back, or sorry, a couple of years back, and now they've kind of given up on such approaches. I don't think there's gonna be a world in which you can use AI to detect AI anymore, at least purely based off the content alone. And I think what the rise of this is gonna be is more verification on all sorts of platforms. We're already seeing a rise of this. LinkedIn is pushing for verified profiles. Twitter or X is pushing for verified profiles.

Aaron Delp (12:20.291)
Yeah, that makes sense.

Rick (12:32.6)
And I think Meta, Reddit, all these platforms, we have a strong belief that's gonna be more important than ever. And for enterprise, I think it's gonna be the rise of phishing. There's gonna be a huge wave of more more phishing attacks. Most, as mentioned earlier, the number one route for insecurity for a lot of these platforms oftentimes is through people. And phishing, I think, is gonna be the primary way. And what we're seeing right now at the enterprise level is many folks are making employees do two -step verification using biometrics, using some form of identity verification.

To a test, that's actually the same physical person get access to these services. So I think that it's going to be what we believe is going to happen. So there's going be more identity than ever because there's just not a way anymore for AI to detect AI.

Aaron Delp (13:15.13)
Yeah. Yeah. And, you know, what you said, it reminds me of, gosh, without giving out too many details about it. So my daughter was involved in kind of a identity theft kind of thing recently. And it was really surprising to me because in order to prove she was her, she had to submit a picture of herself.

She had to submit a video of herself saying she didn't do the thing. And there was all these other steps. It wasn't just your typical, we're gonna send, the credit card companies, we'll send you a thing in the mail and you sign and say, I promise I didn't do that and they write it off. It was very, very in -depth, the steps you had to go through. And I was like, wow, okay. So that's, guess, where we're going in the future now is like.

evidence and video evidence and these other things to prove identity so it's just fascinating. No worries, no worries at all. No, was super fascinating. So let me ask you this though. So let's kind of dig into Persona a little bit. Is it almost like a third party API architectural or stripe of like if I'm a business and I want to do identity management or you know.

Rick (14:10.826)
I apologize in advance, that may have been us.

Aaron Delp (14:36.197)
theft prevention, is basically calling a bunch of third party APIs or like if I'm an architect walk me through what that looks like.

Rick (14:44.74)
so as you were saying earlier, an Uber for X or X for Y, I think that we are very much so similar to a Stripe for identity, a Stripe for X in this sort of case. our two main ways is by API or by SDK. If you embed the SDK, will also perform all the information collection, make sure the data is transferred securely, and then it's collected into the platform. One thing that I oftentimes like to really emphasize is that we're a data processor, not a data controller. So the data...

is doesn't even belong to us. have minimal access to it. It really belongs to our customers. Our general belief is that long term building a single company who, you know, is verifying everybody on behalf of everybody as a data controller. I oftentimes joke I'm not quite ready for such a future yet. It does seem rather dystopian, you know, so I think that the status quo in which

Much like payments, every single company integrates and builds out their own payment stack. However, oftentimes leveraging folks like Stripe, we believe a very similar future for identity, which is we offer the infrastructure for these businesses in which they can architect their systems. Our system will help secure the information, collect it and verify it. And then also manage it as well. So if they want to redact it, it's truly deleted. It's not like replicated anywhere. It's completely wiped. You can set retention policies. You can set compliance policies, consent policies to make sure all of the data for every single different region.

for every single different individual is properly managed and redacted at the right schedule, especially once it's no longer of use. But beyond that, mean, integration is super easy. You can do it via API. So just a couple of lines of code. We oftentimes joke it takes less than an afternoon, especially if you have a stack that can make external API calls, minus all the complex networking. Or even easier than that, SDK. SDK embeddables just maybe 10 lines of code. Drop it into any sort of website out there or within your.

within your mobile application and you can get integrated immediately.

Aaron Delp (16:33.819)
Fantastic. What kind of platforms are you seeing for the most part? it truly like a lot of people are mobile first these days? Like it was in the early days a stripe of like plugging in the readers or what does the, you know, when somebody does do APIs or SDKs, what platforms are they typically targeting to get started?

Rick (16:53.38)
So usually at this point we see deployment across all three platforms in Silent Anity So I'd like to believe it's because our platforms easy enough to integrate with but usually if someone's rolling us out They'll get us set up on their Android app their iOS app and on web all at once

And most commonly the adoption path is by SDK more so than ever the secure management transfer collection of personal information is really complex. So do that safely. The benefit of the SDK is that as an organization, if you're using it, no data touches your core infrastructure unless you want to. it's not like you're collecting, you know, government IDs and like first transferring this into your database before transferring it to us. It's gonna be really complex. It's much more similar to Stripe in this way in which

If you use our SDKs, it bypasses your infrastructure entirely. You can access only the information you want and then everything else kind of handled on your behalf. And, you know, I use Stripe because actually collecting credit card information. Now you have to be PCI compliant. You have to deal with all these complexities. If you're using persona, you don't have to deal with all the consent language. You don't have to deal with all the regionalization of data. All of that can kind of be handled automatically for you.

Aaron Delp (18:04.156)
Sure, sure. And actually that was gonna be my next question is, so based off of that, mean, especially with the regionalization of things, how much of your time is spent building out the systems and how much of your time is just complying to all the different, you know, places in the world that you can have different rules and regulations. It almost seems like super easy for me as a customer wanting to use this, but it almost seems.

super hard for you to stay on top of all of.

Rick (18:35.36)
So that is, I mean, that's a real pain point for us right now. I have oftentimes joked that the real superpower of Persona is not the verification technology, but rather the flexible infrastructure that allows us to dynamically adjust to new regulations. At this point, there's new regulations in every region you can imagine. And the strength of the platform is less so like.

us having to kind of build all this out, but rather it doesn't require a deploy on our side at all and just configurations and allows, you know, we can dynamically modify everything within the infrastructure from retention of the data, where the data is stored, how you, the consent language displayed, you know, like based off the IP of the end user, all of that can be done without any sort of deploy at all. And that really is where the magic comes about. And I think the strength of that is why Persona can work with so diverse industries from many of the largest marketplaces to many of them.

the larger social media companies. We're working with all of these folks primarily because the flexibility that allows us to adapt to the regulations, not only on the regional level, but also on the industry level. Industry level regulations are also really quite the complexity.

Aaron Delp (19:38.868)
Yeah, I can only imagine. Go ahead.

Rick (19:40.492)
So in a weird way, to answer the very, very original question, I would say it's a combination of both. Much of our work these days is actually improving the infrastructure to make it even more flexible. So one of the core kind of benefits of Persona is that I can't tell you anymore where the world's going to move. The world seems more uncertain than ever on so many dimensions, frankly. However, I think that flexibility and adaptivity are the best ways to respond to uncertainty. And I Persona is a platform built with the belief that things are going to be uncertain.

Aaron Delp (20:07.748)
It makes perfect sense. It makes perfect sense. I think that's a great place to end as well. So Rick, if anyone was interested in this or interested in following you and figuring out everything that's going on, where can they reach out?

Rick (20:21.848)
So we're at withpersona .com. You can also always just email me, it's just ricatwithpersona .com. But we're very excited work with customers of all sizes. We work with some of the largest enterprises all the way to some of the smallest startups. So please don't hesitate to reach out. It's been really exciting for us to be able to be on the forefront of kind of what's developing on this space.

Aaron Delp (20:42.78)
Fantastic. Well, Rick, thank you very much for your time. And on behalf of Brian and myself, for everyone out there, thank you for listening this week. And of course, if you have feedback, show at thecloudcast .net is the easiest way to get hold of us. And of course, wherever you get your podcast, if you can leave a review, we'd love your feedback as well. So with that, I'm going to close this out for this week, and we will talk to everyone next week.