

LendIt Fintech



Welcome to the LendIt Fintech One-on-One Podcast, Episode No. 344. This is your host, Peter Renton, Chairman and Co-Founder of LendIt Fintech.

(music)

Before we get started, I want to talk about the 10th Annual LendIt Fintech USA event. We are so excited to be back in the financial capital of the world, New York City, in person on May 25th and 26th. It feels like fintech is on fire right now with so much change happening and we will be distilling all that for you at New York's biggest fintech event of the year. We have our best line-up of keynote speakers ever with leaders from many of the most successful fintechs and incumbent banks. This is shaping up to be our biggest event ever as sponsorship support is off the charts. You know, you need to be there so find out more and register at lendit.com.

Peter Renton: Today on the show, I'm delighted to welcome Rick Song, he is the CEO and Co-Founder of Persona. Now, Persona is in the hot identity verification space, they have a number of fintech clients, some big-name clients that you would know, we talk about some of those in-depth. We also talk about the identity verification space in general, how Rick believes it should work, how they differentiate themselves from their competitors, we talk about the different use cases, we talk about data storage.

We talk about the customer experience and how the expectations have changed there and the tension between friction and providing a good user experience and why really Rick believes in a real flexible, personalized approach there. He also provides his perspective on the recent fracas with the IRS and their facial recognition software, what the IRS did wrong and what he would have done differently. We talk about the arms race with the fraudsters and how that's been going and much more. It was a fascinating episode. hope you enjoy the show.

Welcome to the podcast, Rick!

Rick Song: Hey, thank you so much for having me, Peter.

Peter: My pleasure. So, let's get started by giving the listeners a little bit of background, I know you spent some time at Square and just tell us a little bit about what you did there and then how the idea for Persona kind of came about.

Rick: I was an engineer at Square for about five years, not the most exciting background, but nonetheless the entire time there I was focused on working on identity there and one of the more fascinating things that we've encountered at Square, Square started off as a payment solution really focused on merchants, enabling, you know, fast, seamless payments anywhere, but over time, Square has evolved. These days, I mean, Square has evolved so much that the name itself is no longer Square. At that time, it was evolving from starting off purely as a

LendIt Fintech



payment processor for small merchants into an entire suite of products for small businesses, anywhere from lending to payroll, fulfillment.

Back then, once upon a time, Caviar was part of Square, to Cash peer-to-peer transfer and now, these days there's investment, there's Bitcoin, there's crypto, there's so much on this platform, but one of the core things that we were encountering at that time was that identity was starting to emerge in different ways for every one of these use cases. If you are someone who is signing up for payment processing versus you're getting a million dollar loan, the core or kind of like identity experience started to change, what you need to know, how you need to know them for both a compliance, a fraud, a risk perspective, all these things were starting to kind of change.

Now, on top of that, we were building not just a single, one-time relationship with these merchants, it's certainly a lifelong relationship, we're powering their business, we're working with them for possibly decades to come so in that perspective we were starting to see identity emerge from this one-time transaction and evolving into a relationship instead.

So, these were really the two core kind of seeds for Persona, first of which identity was starting to bifurcate from being this one-size-fits-all into an entire ecosystem of every single experience really necessitated something different, from lending to payroll, from signing up for compliance purposes to peer-to-peer money transfer. And two, we're starting to see identity evolve from this one-time transaction into need to know who this person is across the entire relationship with them and those were really the two core foundations around Persona.

What we've seen in the market this time is there are a lot of really, really great point solutions, they're lawful, it's out there, we're building, you know, solutions out there that really look at identity from a singular perspective. Either one, from a methodology perspective where they're focused on like saying that file measures the future of identity, that is what is going to be what solves it all or two, we're starting to see folks who are really just focused on a single industry, they're like, you know what, we're just KYC and KYC is what we do.

At Persona, we really took step back, like how do we build a platform that would be universal, that would work for any use case and not just that one time transaction, but rather ensuring that there's this level of trust between the user and the organization across their entire....so those are really the two core things behind the background of it all. We touch a little bit deeper in terms of like the background on the industry side. One core thing that we're also really starting to see is that as identity becomes increasingly important for different businesses, more folks out there are taking a maximal approach towards collecting as much data about the individual as possible and we're starting to see this increasingly become more and more uncomfortable,

Peter: Right.

LendIt Fintech



Rick: You know, you will ask folks like ten years ago, we would say, SSNs, we probably all felt relatively uncomfortable bringing our SSNs online, but these days we're collecting things like biometrics and collecting some other ideas and it's becoming increasingly the norm. I suspect that, given the trend that we're seeing, this will only continue to increase and as much as I want to believe that there's going to be some silver bullet towards solving all these, and if there is, we're going to be on the forefront working hard with companies to make sure that we are making this successful for all. My perspective is maybe the faster way to get us into a place where we're just being not as aggressive is not only tailor it for the business, but also tailoring that experience for the individual.

If you're a low risk individual, if you're someone who, you know, is verifying yourself from your home on a device you've used countless times, we should lower that friction making sure that you're not submitting as much. Maybe we don't need a biometric, maybe one can submit an ID, maybe it's just her name, birthday and address, we're going to have enough certainly that you are who you say you are with just that. Versus, if you are, let's say, traveling to Russia, you know, it's a one week trip, somewhere far off, if you have to access the Internet through EFTN, we're not saying it's not you, we just think that, you know, for both you and the business security maybe we should collect a little bit more and like making sure that that experience is tailored for every individual.

This isn't just on a risk perspective and from a background perspective as well, you're a recent immigrant, it doesn't make sense to collect your SSN, you likely haven't gotten one. If you are, you know, from a lower income using credit headers as a mechanism to verify your identity, it totally doesn't make sense. So, Persona is really trying to take this idea that there is no one-size-fits-all and businesses need to know continuously that people are who they say they are.

Peter: Right, right, okay. So then, maybe can you just talk a little bit about some of the fintech companies that you're working with because I've seen in the press some of the...it's some pretty big names that you have as your clients that are out there publicly, can you just take us through one or two of those and describe exactly what you're doing?

Rick: A couple of which I've always loved to call out are like Square, Robinhood and BlockFi and BlockFi is one which I really love to call out because they're really on the bleeding edge of identity. They're within the crypto space and crypto and fintech, they're such an interesting kind of just connections here, right, but at the highest level I'll start with Square first, this one's going to be a little bit shorter.

Right off the bat for Square, the first major use case we worked with them on is PPP so at that time we need fast distribution, millions of Americans needed access to PPP loans is just the scale fashion and one other core thing for Persona is not only do we care a lot about flexibility to make sure that every one of these folks out there could have access to these highly critical loan,

LendIt Fintech



we also care a lot about privacy and automation. And we think that, you know, these days we think a lot about automation from the perspective of cost cutting from a modern and advanced perspective, but we really felt that automation also unlocks privacy and ensures that there isn't someone in a foreign country looking at your IDs manually.

I personally believe that the future of privacy will not be that, I think that there is no way that we continue down the track of there's so many reviewers of every single thing, especially those not associated with the business that you're doing business with. I cannot imagine (garbled) we built this in a fully automated way. The benefit of this is in this height of the environment we were able to partner with them making sure that every single loan which they will do will be done in an entirely timely fashion. PPP evaporated in a matter of moments.

Peter: Yeah.

Rick: And then on the BlockFi side, this one's really exciting because BlockFi is really evolving the same way that we saw Square evolve from starting off as, you know, really leveraging crypto as a mechanism for savings, for investment into an entire kind of crypto ecosystem. Financial wallet (garbled) it was super exciting, we worked with them on all stages of the lifecycle so earlier I used one which really focused on Persona like tailoring that use case. I love to use BlockFi to talk a little bit more on the relationship side. BlockFi, if you start opening an account, you're going through Persona, working with us and help the individual set up for continuous monitoring making sure that the transaction that this individual opens continues to stay safe. They're using us to track and make sure that hey, this individual isn't trying to, you know, transfer money, they're not trying to do suspicious activities with their crypto account.

You're trying to recover your password or you're trying to do a major withdrawal, the risk is sufficiently high, they're leveraging Persona to make sure that it's the same individual who is using this money. One of the mysterious things, especially in the (garbled) further and further away from bank account, it also oftentimes means it is a little bit harder to ensure that the money is going to exactly the right person, the reversibility of crypto has always been (garbled) parts of it.

So, we work with them to ensure that the safety of the transactions are there, we help them also gather additional information if some person is doing high risk stuff and we need additional documents beyond those that might be (garbled), we help them collect these information to make sure that this person's still doing the right stuff there and as we unlock new account features as well we're all there along the way making sure that, you know, you're constantly building that relationship with this individual. One benefit of this is it also ensures that you're not cuffing everything right off the bat, right, you do not just ask for the entire kitchen sink, entire background, just collecting a sub-set of information.

Peter: Right, right, okay. So, and you mentioned Robinhood as well.

LendIt Fintech



Rick: I'll be honest, I can't go too deep on their end. For them, one of the more exciting things is really just making sure that when you sign up a higher risk individual, you're going through Persona on these cases and if you're selling, you know, for tax, for property or if you're trying to focus a little bit more so on these high value transactions, Persona is there to make sure that you're buying a million dollars of G&P stock, I'm not saying you can't, you just have to make sure that it really is you wanting to make that transaction.

Peter: Right. I just want to go back to BlockFi because I'm a BlockFi customer, we've had Zac Prince on the show, the CEO there, and really an interesting company. As you say, they're in the crypto world where a lot of people like to remain anonymous, what is it you're actually doing, if you could just maybe dig in a little bit and tell us. If I want to go and like clean up my entire BlockFi account, sell it all, what are some of the things you're going to do to verify that I am who I say I am?

Rick: It really depends on the risk that they're seeing on your end, right, and there's a lot of things that factor into that risk. This could be anywhere from the amount of money withdrawn to the location you're withdrawing it from to the additional risk scores, your prior activity could be on the platform itself and depending on all these different criteria, what we're presenting is something that might be a little more unique towards the exact flow you're trying to go through. So, this could be collecting a biometric, making sure that, you know, you're asking for a selfie, making sure you are who you say you are in that perspective and comparing that against prior incidents, asking for a little bit more personal information, asking for some government ID again and any mix of these to kind of just get that additional certainty that you are who you say you are when you're kind of like making that major withdrawal.

So, we're doing things like these especially kind of like add that additional certainty on the risk. One of the cool additional things is also taking it to a level like discuss these identifiers as well from device information, earlier I mentioned kind of location information to kind of compare hey, is this close to the previous time that you were on this platform and utilizing all of that to kind of give a holistic perspective as to is this person who they say they are.

Peter: Right, right, got it. So then, you're taking all of this information, how are you storing it like particularly biometric information or I'd say all of it, like what are you doing? You, obviously, have to take it in, you have to put it somewhere to compare it to what you have then what happens, where does the data get stored or do you just delete it?

Rick: The answer here is it really, really depends on the use case. So, we're partnering up with folks too for alcohol delivery for check-ins as well and depending on the use case, as to whether we have to store or not, really depends on the compliance and the organizational controls. So, I'll speak on this from two perspectives one of which is when we start into this, how do we store it. So, on the when do we store it, it really depends. If you're a financial institution there's a lot of

LendIt Fintech



regulations in terms of how long we have to persist these data, for most financial institutions there's far as a minimum of seven years to store these data because, you know, for regulators, if you come in later on to see what's going on, they need that data to be readily available.

On the flipside, this doesn't apply to all information so, for example, for biometric information, oftentimes what we'll do is we'll discard the biometric markers. The markers themselves are oftentimes the most at risk information so after the comparison is made, we discard the information and what we generate the next time that you need to verify yourself again.

Peter: Okay.

Rick: If anything is kind of hijacked, they're not hijacked in the most sensitive aspects of how is comparison to be made.

Peter: Right, right.

Rick: On the second half is how we do store it. On the security aspect, we're trying to do a lot and fortunately, my Co-Founder and I come from Dropbox and Square, respectively, and a large portion of this team really comes from our backgrounds at Square, Dropbox and a lot of folks who have like data infrastructure and data security for a long time and one thing we always like to call out is that storing data securely is not an intractable problem, it's actually a very, very tractable problem. My favorite analogy here is you just think back on when was the last time that you've seen this major payment giants leak credit information. There's a lot of security being applied and the reason why is because there's been a lot of regulatory and compliance requirements to actually manage these data whatsoever that adds this requirement on businesses.

But, two, it's also just because these companies have a tremendous amount of intent to manage these data well. At Persona, I mean, this is the lifeblood of our company, managing, collecting, verifying these data on our customers' behalfs so we try to apply a lot of similar techniques that we've developed at our previous roles to ensure that all of the data that we're collecting is managed and being stored in the best way possible.

Peter: So, you know, we're recording this in mid-February and in the news, I think it was early this week, the IRS came under fire because they were using facial recognition software because, they said, there were a lot of people who were getting through some of their fraud detection. They were having problems with verifying peoples' identities so they put in facial recognition software and then people said, oh no, no, you cannot do that so I'd love to get your thoughts on the story, what should the IRS be doing?

Rick: My perspective is really threefold, the first of which is I think I should be opt-in. Honestly, the answer here is like not everyone's adjusted, well, really, really the struggle there is that

LendIt Fintech



everyone has to do it, I didn't get a choice and I think that's a really big problem and our perspective on it is that every individual, they should be able to choose how they need to build that level of certainty and there should be the alternative mechanisms that have to always submit a biometric and this isn't just from a privacy perspective.

Another very, very real problem of biometrics too is accessibility, right, if I recently, you know, had a tremendous change in appearance, it's going to really affect my ability to access these services and for something as critical as the IRS did not have that back-up flexibility I think is a really, really good chance. The first, of course, is that opt-in aspect and making sure that biometrics isn't the keys to the kingdom, but rather just one of the many kind of paths you can take.

Peter: Right.

Rick: The second is I think the overall approach that was taken, it's collecting everything possible for every single person. Earlier, I've been speaking a lot about this idea of progressively segmenting individuals based off the risk that they present to minimize how much they were collecting. My hope for the future is not one in which we're collecting more and more just to keep reaching that same level of assurance that individuals are who they say they are, but rather we're seeing a future where depending on who you are, minimizing that risk and my favorite analogy on this stand is really again back to payments. You may see this as a recurrent theme because half my brain, given my prior experiences, will always be on the payment side.

In the payment space, when you make a really large and maybe a risky transaction you'll get a call from your bank and they're like hey, can you confirm this transaction, right, they're not doing it every single time, only when there's the highest risk they'll be like hey, I just need, you know, click below after the information about you to make sure you can make this payment because this is a very novel one, maybe you're buying a Tesla in Florida, who knows, right. I think identity sites should be the same where look, if you're signing for the IRS, you know, you're on a VPN, you should probably do something more, that's a really, really risky kind of interaction, it's fascinating, you know that you need to be getting access to the IRS site, you should do something else.

Peter: Right.

Rick: The third point I have on the rollout is I think you really need a data processor there not a data controller and this is getting a little bit too much on the GDPR terminology so what I've really kind of like break it down into is as a data controller is you're building a relationship with a private company, the private company owns your information and that's delegating that back to the IRS. Whereas, at its core, the information that you're submitting should belong to the IRS, that's who you're building the relationship with and it's a little bit strange from my perspective to have to kind of like have this middleman who is just telling the IRS you are who you say you are,

LendIt Fintech



but that's not who I trust to mediate, right. I want to build a relationship with the IRS in this case, I want them.....I trust the government, I may not always trust a private company so I think this is like the third kind of aspect. What we really need in that kind of situation is that infrastructure could provide the IRS the tools that they need not a proxy that I'm trusting for some of the most sensitive information for access to that,

Peter: Right, right, that makes sense. So, it leads into my next question which is I want to get your sense on how customer expectations have changed, particularly when it comes to sort of the experience of opening up an account or making a big withdrawal because there are more customers now online, you know, in the last two years than there ever has been before and so more people are having to come up against all this. So, how has customers' expectations changed over the last couple of years.

Rick: I'll say it from two ends, one of which is kind of for our customers and, of course, the second is customers' customers, the individuals like all of us, we're going through this and for the latter what we're really seeing is we're expecting different things from every experience. I think that's really fascinating so I'll break this down a little bit. These days if you are, let's say, opening up a bank account, it's probably an expectation to submit your SSN, but if you're completing a course on Coursera or Udemy it'll be a really weird experience to submit your SSN.

Peter: Right.

Rick: On the flipside, submitting your driver licenses is still a little bit kind of sensitive if you're opening up that same bank account, but if you're ordering alcohol there is literally no kind of sensitivity around submitting driver licenses, this is how you've been buying alcohol in person for our entire lives. So, what we're really finding from consumers these days is that they're expecting different things based off experience they're really signing up for, there's like these embedded expectations around it and this is one of the major trends that we believe is fighting against this idea that there's going to be a one-size-fits-all, a silver bullet for identity. It's this idea that consumers expect unique identity experiences, depending on what they're interacting with. If you're opening up a BlockFi account versus if you're opening up a JP Morgan account, consumers implicitly expect a different experience for the two of them.

Peter: Interesting.

Rick: And, then for our customers, what we're really finding is organizations will provide these experiences. For every challenge in the identity verification space is I don't want fraud, but I don't want a maximum conversion and, unfortunately, the history of this has been look, if you want to fight out more about fraud, you're going to sacrifice some conversion, you want more conversion, you've got to let a couple of more bad actors through. Our perspective on it is you can have both, it's a lot more work to have both, but the way you have both is by, again, tailoring

LendIt Fintech



that experience to the individual. So, for us, we're really trying to push on that angle of tailored experience, make it kind of progressive, make it tailored for every and unique experience for every individual such that that way high risk decrease the fraud and then if it's a lower risk, increase the conversion.

Peter: Like there is that friction that always seems to come between a good user experience and preventing fraud so what you're saying then is you isolate who is the low risk, give them as a seamless an experience as you can and if you're someone who's high risk then you'd have to go through more hoops so it sounds like you have to obviously determine early in the game who's high and low risk, right?

Rick: Our actual perspective on this is you can do it from that progressively so not only just right off the bat, right. I think, historically, within the space it's always been give this person a risk score and then we kind of like bifurcate them in this way, but this age where we actually find it to be even more effective is to do that while they're going through the experience as well.

As you get more information, that information helps you actually even ascertain with more certainty whether this individual is risky or not so a really, really kind of basic example of this is if someone chooses to take a photo of the government ID versus upload a photo. Uploading a photo, for better or worse, is a bit higher risk. If this photo's been passed through a photo editor that's probably high risk, they could just have been cropping it, but the fact that they touched it with one presents an even higher risk than a photo was just freshly captured and even more so than one that is auto captured.

Peter: Interesting, okay. I've got one in my computer and I cropped it and didn't realize I was adding to my risk level there (laughs).

Rick: I'll be honest, on the cropping side, we can detect that so we generally won't increase your risk there. We can also detect if you had decided, you know, to do some additional touch-ups from a coloration perspective and in those type of cases we present that as a much higher risk than, you know, I'll probably attribute that as almost like a zero....

Peter: Right, okay, okay. So then, I really like your approach, I think it's really interesting how you're kind of making this sort of custom, but then does it vary then when in the process people are going to have to prove their identity. I mean, is this something that if someone is opening up an account, do you decide or does your customer decide because eventually you'd have to prove that you are who you say you are. What's your thoughts about when that should happen?

Rick: Our perspective is we partner with the customer and we will help or protect them when we know exactly what makes the most sense for them and it really, really will vary who the customer is and like what kind of experience they want to offer because that core identity is foundational to the product experience. For a lot of these types of businesses, it isn't just some

LendIt Fintech



check what they're going through anymore, more so than ever identity is a critical aspect of their entire product experience for their customers.

So, for us, we fundamentally view ourselves in the stamp of we are a data processor, we are there to help you build that infrastructure, we oftentimes make the analogy that we're like AWS, we're like GCT. We're not here to like take over your business, we're just offering you the tools to build your business on top of, but at the end of the day it's your data still and it's your processes that you want to help.

We're here like eight of us consultants to help work with you, to help build out and introduce when you should be using this the same way that AWS might be working with you to figure out when you should be using their best three tools, their scores tools, their networking computer tools. We're here to tell you hey, you may not need a biometric here, it might be a little bit overkill for the experience you're trying to offer, maybe you actually should...lean a little heavier on your own passive identifiers, that way you're not collecting so much sensitive information from the individual, but at the end of the day, it really is up to the customer side when they want to introduce this because we fundamentally also work with you, identity is foundational to the process.

Peter: Right, okay. So then, let's take a step back for a second and talk about sort of the race or the battle, shall we say, between the fraudsters and people like you. How are you staying ahead of the game because they've got all the same technology that you have, right, they've got good technology, they've got good people working for them, how do you stay head of the game?

Rick: So, I can't disclose too much on this side (Peter laughs), but just the nature of it, right. Earlier, talking about kind of our detection on photo technology already, I was already a little bit like I suspect we might start seeing it increase in live captures and fraudsters would be aware. My perspective on this is that there won't be a single technique anymore, we've been hunting for so long, but there are so many cases now and it's harder and harder actually to be a fraudster these days than ever before, assuming you're implementing this well.

The reality of this, you have to watch for so many different things from your behavioral network, device, you know, every aspect of this there's a bunch of different signals that we can collect and if you're not careful you'll trip one of these, each one of these will have add any roadblocks. So, our kind of perspective on this, while we're trying to find something, you know, on for that next thing, take all of the different tools that we have today, consolidate all these in, it's just harder than ever before, right, increase the amount of friction. They really have to go through all those hoops and hurdles that they have to jump through to really be able to impersonate a good actor.

LendIt Fintech



Peter: Right, right, okay. I want to talk about your investors, you've got some pretty major investors on your cap table. I know you recently, last year I guess, you became a unicorn, tell us a little bit about your fundraising journey.

Rick: We raised our seed round with First Round Capital and that was our initial round way back I think in the end of 2018 and after that we raised with Coatue, I think we're one of their earliest Series A investments at that time. We partnered with them because of my prior relationship actually with Andy Chen, who's one of their GPs these days. One core thing for us at Persona around investors has always been really focused on who we're working with rather than the firm itself and, you know, rather than like the reputation or even like the valuation of the price. We've almost taken a pretty significant haircut at every single fundraise to make sure that we're leaving some money on the table in goodwill and also making sure we're working with the right folks so both for First Round and for Coatue.

The folks that we end up working with were folks that we've had established relationships or it was a heavy reference from a very long term established relationship with. Since then, we've raised both a B and a C, our B was led by Index Ventures from Mark Goldberg who was formerly at Dropbox, you're seeing that trend coming again where he was at Dropbox along with Charles. I've known Mark since our seed round, he's one of the earliest folks we spoke with and was one of the best folks we've had contact with and then later on, the Series C, led by Founders Fund, Keith Rabois over at... an ex-Square as well as Napoleon who joined our board, again, heavy reliance on relationships, on trust in the same way that we're trying to facilitate that trust with our customers, we try to kind of bring that in as well.

A lot of these was brought on from the advice of Jack at Square when I first left, had a series of embarrassing questions to ask of these days, I think that comes from experience then. (Peter laughs) I can't say I'm proud of how it was, I did not know how to interact with him, you know, he's a monolith of a person so I've come in prepped with a bunch of questions. His answer to my question about fundraising was incredibly insightful and what he had said that time was investors are employees that you can never fire so think wisely and we really kind of took that to heart to make sure that the folks we're working with are folks that we want to work with for years and years to come.

Peter: Right.

Rick: I mean, the only other thing I'd say here would just be that for this past, maybe five-ish years, valuations are through the roof. I mean, we're all seeing it, right, the multiples, what we're seeing on the market, for better or worse, it is easier than ever to fundraise, but my personal perspective is this probably won't last forever and making sure to really leave some on the table, this is why our perspective. On every single round that we've actually had to date, we've actually left a significant amount of valuation on the table making sure that look, we are also

LendIt Fintech



leaving some room here to kind of demonstrate like we're in with you all, like we're going to be here throughout bigger funding.

I think that's really, really critical these days to be a little bit more prudent in terms of what we're chasing for because, you know, every start here isn't trying to build a company here like trying to have that quick exit, we're all here to really build generational businesses, kind of those that will stand the test of time and making sure that in the same way that, you know, these relationships with investors are long term relationships. That means also we help make sure that the actions we take are really thinking about that long term as well.

Peter: Right, right, okay. Let's close maybe with this question, I'd love to get sort of your vision for the future of identity verification. What do you think it's going to look like in the long term?

Rick: It's an ambitious vision that we have, I hope that the future of identity verification is one in which we're submitting less data and I'm hopeful that the way in which that can happen is really through that risk segmentation. By submitting less, it also means that the data that whenever we really have to submit is isn't just compromise, right, the reason why I think these days it's so, so, so terrifying is while we're submitting more and more data, we're also compromising ourselves every single time. As we try to seek these higher risk assurances, we're simultaneously undermining the very foundation for the identity infrastructure out there. Every time you submit a government ID, for better or worse, that information is being spread to somebody else and that's another target that can be compromised.

So, on our end, number one, we want to make sure that every company out there is building on top of secure infrastructure such that they don't have to manage that data themselves in the same way that today, businesses are building their own cloud data centers, they're relying on folks like Google, like Amazon, we think that future will be that hopefully, most businesses out there aren't managing that most sensitive data themselves, that they can rely on secure infrastructure, it's still their data, but they can rely on the storage of someone who's 100% focused on managing these data well such that these data doesn't get compromised.

And two, by making sure these data isn't compromised hopefully, the future also is that we don't have to submit it nearly as frequently and only whenever we really have to, when you actually have to kind of put these out there. So, we think that the future of it will be one in which there'll be less data out there, less data compromised. The way in which to unlock these is by making sure that we're not submitting it every single time by minimizing the amount of data that they're submitting today.

Peter: Right. Well, I hope you're right, it's going to be interesting to see. Rick, I really appreciate you coming on the show today.

Rick: Okay, thank you so much again for having me.

LendIt Fintech



Peter: There are two things I want to highlight that I thought were really interesting there. One is what Rick was saying about the fraudsters and how they really have a difficult time today, it's much more difficult to be a fraudster than it ever was before. Now, admittedly their tools are better as I said, but we have such sophisticated tools now to detect anything that is out of typical behavior than outside the norm so it is getting harder and I thought that was a really good point.

The other point that he made right at the end there was just trying to store as little data as possible, trying to ask for as little data as possible. I really like the approach that Persona have of trying to really make it so that every client is different and every journey can potentially be different because we want to make it easy for the good guys and just really, really hard for the bad guys.

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

(music)