PODCAST TRANSCRIPTION SESSION NO. 204 - HUSAYN KASSAI

Welcome to the Lend Academy Podcast, Episode No. 204. This is your host, Peter Renton, Founder of Lend Academy and Co-Founder of the LendIt Fintech Conference.

(music)

Today's show is sponsored by LendIt Fintech Europe 2019, Europe's leading event for innovation and financial services. It's coming up on the 26th and 27th of September in London at the Business Design Centre. We've recently opened registration as well as speaker applications. You can find out more by going to lendit.com/europe

Peter Renton: Today on the show, I am delighted to welcome Husayn Kassai, he is the CEO and Co-Founder of Onfido. Now Onfido are a fascinating company, they have become almost the standard now in identity verification for the fintech space. Certainly in the UK and Europe, they are used extensively and becoming more so in the US, but anyway, I wanted to get Husayn on the show because they are really doing interesting work.

I wanted to talk about how their system works, what's wrong with identity today, why the current system is so flawed, we talk about the challenge of user experience and reducing friction, we talk about how banks are using this, we talk about artificial intelligence, and how that is playing a major role in improving these models, and we talk about what it would take to actually have a perfect world with very little identity theft. It was a fascinating interview, I hope you enjoy the show.

Welcome to the podcast, Husayn!

Husayn Kassai: It's great to be on.

Peter: Okay, so I like to get these things started by giving the listeners a little bit of background about yourself and...you know, you haven't had a long and storied career because, as we were just chatting before we hit record, Onfido was your very first job out of college. So maybe just tell us a little bit about why you decided to do that instead of going and getting a job and what are some of the things you studied in college that you felt prepared yourself for this.

Husayn: Of course, so in my last year at university, I was fortunate enough to be the President of the Oxford Entrepreneurs Student Society and during that whole year, I got to see very many startups coming and pitching and presenting and asking for funding so I got to learn quite a bit during that process. We had a clear metric...my Co-Founder later also was the Vice-President of Oxford Entrepreneurs at the time and we had a metric around wanting to see how many successful spinouts we can have.

Despite us doing a lot of activities and trying very hard, towards the end of the year we still only had maybe one or two actual startups spin out and do it full-time. So we had learned so much and we genuinely felt that there is a big need to solve this identity problem that we felt that we should do it ourselves because the norm is you kind of have to conform to expectations, you know, you go and earn a salary, you have a to get a mortgage, you have to tick these boxes. We had experience and we saw that counter to what the expectations are, doing a startup is never necessarily, there's never an ideal time for it. The ideal time is when you see a real problem and you feel like you can work to solve that so we felt it was the right time and that's why we went straight into getting the company going.

Peter: So then what was the thing you saw that led you to the idea that became Onfido?

Husayn: So fundamentally, it's about building trust and Onfido in Latin is a mix between fido which is “trust” and confido which is “confidence” and we saw that the way that identify verification process was carried out was essentially what we had deemed as broken.

We have our different stories as co-founders, but when I turned ten, my parents moved from Iran to the UK and I remember quite well that it took them a few months to be able to open a bank account in their own name surely because they weren't registered on the credit bureau. Growing up, I found out that credit bureaus essentially had a log of everyone’s date of birth, name and address and it excludes half the world of the adult population who are underbanked, unbanked and are therefore not on the credit bureau so it has an exclusion and access problem.

On the other hand, you have a security problem whereby almost all of that data is already breached and in the dark web anyway so a bad actor can just steal your date of birth, name and address and open an account so you don't get security and this kind of loss of currency. So given that it was excluding a lot of people and also not offering security. We felt sure there was a much better way as the world is moving online for businesses to be able to verify their customers in a user-friendly way, but also secure and to give access to as many people as possible. That was the initial mission which we've been working on now for seven years.

Peter: So tell us a little bit about those early days. I'd be curious to sort of get your take on did you have a particular product in mind when you launched, were you trying to sort of redo the entire process? What were the early days like?

Husayn: So when we looked at how are you able to prove someone's legal identity, we first distinguished how we are going to focus on your legal identity. So we could see how Facebook has standardized the way everyone shares their social identity, your likes and preferences and so on and how LinkedIn has solved the problem of everyone who ever wants to with an account be able to share their professional identity, your academic career or job career and so on.

So our focus was on your legal identity, that is your date of birth, name and address so that you're compliant if you want to carry out some financial transactions, sign up to a lending platform or similar and then at the same time if there is a breach and a bad actor is found, then law enforcement can be told precisely who they are so that was our focus around legal identity.

Our third co-founder, Ruhul, is our technical co-founder. His university thesis was using computer vision and machine learning to spot wildlife in 25,000 photos of the jungle so this pattern recognition research that he did, we felt very well mapped on to government ID checks. So when you want to open a bank account, for instance, you go in person and there is a bank clerk and an individual that asks to see your passport or driving license and deems it to potentially fraudulent or not and then compares your face to the photo on that.

With our technical co-founder's research, we could see that we could bring that bit and make it digital and bring it online so not only is it more secure, but it's actually a lot more convenient too. So that was the first version of the software and naturally, we've been improving it ever since.

Peter: Okay, interesting. So then what is it that is specifically wrong today, is it just merely the fact that your data is out there to be stolen, is it the fact that really we're looking at, you know, a system that…it's all about these legacy products like a driver's license or a passport, is it merely the fact that these things are so easily stolen, is that the biggest problem?

Husayn: So there are a few and identity fraud, as you say, is a big one so in the US, for instance, it's the largest crime and the fastest growing crime across all of fraud, specifically online frauds. The common denominator is identity theft because a fraudster does not want to get caught so the first thing that they do is impersonate someone else, or come up with a fictitious identity so that they're able to commit a bad act.

It is a large and growing problem because 2 to 5% of the world GDP is laundered money, that's between $800 billion and $2 trillion which are United Nations figures so it's a real shame that less than 1% of that is actually caught because money laundering is used for human trafficking, drug trafficking, terrorist financing and so on so not only is identity theft problem a large one, it is getting worse. When you consider the reason why it's so bad and getting worse is because the current systems in place to address it aren't fit for purpose.

On the one hand, you have the option of going face-to-face in a bank branch and being verified, but as we know, that's not accessible to everyone and most consumers now prefer to do things digitally and online and there is a big convenience factor that is the driver. But on the other end of the spectrum and the other approach is to verify people online and online verification, historically, has been predicated on using credit bureaus and that credit bureau model is just a centralized database, but because it's leaked or because it's been breached, that data is accessible to bad actors and hence, it has lost its currency.

So there are one or two other sort of smaller alternatives, using social media which has a privacy issue and sort of is not seen as the right thing, nor should it be, or using knowledge based questions such as, you know, what's the third character in your last utility bill for instance, which again has a lot of friction because users aren't necessarily accustomed nor used to storing or saving or looking up utility bills.

So our approach, which was from the outset focused on a user showing their government ID, either a photo or a recording of their face, was designed so that we could do a very good job of determining if it's fraudulent or not because we run our machine learning models on whether that government ID is fake and then secondly, whether the person showing that ID is the owner of that by taking a photo of their face and comparing it with that. So that’s our problem, is identity theft, the current solutions are in our view, are not fit for purpose. Third, is that the world is moving online and businesses no longer see their customers face-to-face, and hence they need to have this in place.

Peter: Right.

Husayn: So we have four building blocks that we focus on which is fundamentally to help the 98% easily access services; second is to get very good at determining which 2% are the bad actors and they are two sides of the same coin; the better you become at detecting fakes, the more easily you can onboard that 98%. Third is to uphold privacy, and fourth is to make it as frictionless as possible so it is an easy and friendly user experience. That's been our chief focus to solve this identity problem.

Peter: So then take us through a typical example of how your product is implemented. I know you've got several clients in the fintech space and the banking space, but let's just go and take us through...someone is opening up a new account, let’s take LendInvest, for example. I listened to a podcast where you were on with I think it was Christian Faes of LendInvest so I'm an investor, I go on to LendInvest, I open an account and then what happens as far as the verification, what are you doing?

Husayn: So as part of the registration process at LendInvest, you either, on the portal or on the app, at some stage, probably stage two or three after you’ve entered the fact that you’re interested in taking out a product and so on...that's the point at which our SDK kicks in. Essentially, it’s an experience where you are then asked to take a photo of your government ID, it can be a driver’s license, passport or similar and then once that is done the next stage is to take a photo or a short recording of yourself.

Once you click you're ready then you hold the phone or it can be your webcam on your computer for instance and you're asked to read three randomly generated numbers so for instance you would read 2,5,6 or whatever the numbers happen to be and you're then asked to carry out a task. It can be turn your head to the left, turn your head to the right or something simple and then you click submit and that's it.

We then take it from there and then the checks are processed and the results are sent via API to the team at LendInvest, but behind the scenes what’s happening is when we have a photo of your ID like your driving license, we have seen tens of millions so we know what patterns to expect, we know what fonts, characters and if it has been digitally tempered with and so on and so forth.

So the machine learning models can determine whether it seems fraudulent or not and secondly, the photo on your driving license is compared to the face that you took either a photo or a video of and we can sort of determine if you're the same person or not so that LendInvest would know that, not only has a person been verified, part of their KYC or Know Your Customer checks, but the person presenting the details are who they claim to be and the actual owner of the identity.

Peter: Right, right. So then how confident are you…is it 99.9% confident that the person who owns the ID is the person, particularly if you're doing a video, I imagine video, particularly if you ask them to do a task, I mean, I can't imagine that that could be hacked very easily, so how confident are you that you've got the right answer whether this person is who they say they are?

Husayn: So in some ways we're kind of like an anti-virus software where there will be sophisticated fakes that cheat the system. So what we're able to do is two things; one is to say we are significantly better than manual, human teams doing it, either comparing templates or in person and secondly we're better than any other digital offering.

The reason for that is because of the machine learning models whereby as an ID comes through if it's fine then it gets processed, but if we suspect that it might be fraudulent..for example, a password image might be stained. Now when it's stained we have fraud experts that double check and when the fraud expert double checks, they'll be better able to determine is it stained because it was accidentally put into a washing machine or does this look like a sophisticated fake pattern or anomaly that we've seen in the past and therefore, it is scored accordingly.

So a client typically, let's say LendInvest would get 90% coming back as fine and then about 5% would be classed as consider. So either it's because it's a black and white document or it's expired or a number of different reasons and their team will double check and every business has its own threshold as to what they would or wouldn't accept, but these are triggers for them to be able to double down and focus on the 5% to be able to automate the 95%. And then 5% are typically rejected, either the person has not been able to effectively upload or they've stopped the process or something similar.

Once businesses integrate us and they compare their metrics prior to them integrating us, they can see the fraud rates going down sometimes in a pretty substantial way. So Zoomcar, for instance, which is the largest peer-to-peer car rental service in India, their car theft halved once they integrated us. So some of those 5% that drop off, they can do so as a result of legitimate reasons, but some may be bad actors that is because they don't want to expose themselves or because they know there's no way to cheat the system then they essentially self select out.

Peter: Interesting, interesting. So then...I keep thinking about, you described that process and...how do you think about the friction? There really is friction between a good user experience, a seamless user experience and going through this identity verification because the person sitting at the computer...I know I'm a good guy, I shouldn't have to go through all this rigmarole, particularly if you're not all that adept at using your cellphone. How do you approach that?

Husayn: Most people tend to expect to have to go through some sort of compliance check, especially if they're asking a financial service, particularly if it's lending, so part of it is because it’s integrity in the system...if it's very easy for people to come and borrow money, we're doing very little checks then naturally, you might get the impression that it's easy equally for bad actors and therefore, the platform can not sustain itself.

The best thing with the wave of fintechs that we've seen is fundamentally...I mean, lending has happened for hundreds if not thousands of years which as you know better than I for example, but more recently what the fintechs have been able to do very well is put the customer experience at the heart of everything that they do and as a result, they are able to operate digitally or fully online and as a result, we from the outside have had to adapt and focus and partner because we also were aiming to make this as easy and frictionless a process as possible.

And so when it comes to showing your ID and a photo of your face, the good fortune is that smartphones and other technologies have now in many ways normalized it, especially taking a sort of a selfie or a photo we often...more and more of us are now using it just to unlock our phone. So because it's been normalized and because more and more consumers are seeing this repeatedly every time they're using one of the large fintechs or rental car services or online communities they’re seeing us so it's in many ways normalizing. Does that help answer the question?

Peter: Yeah, that makes sense. So how long does it take typically, what’s the average user time like they get into your system, they've got their driver's license, they’ve taken a photo, a selfie, is this a 30-second process, a 90-second process? What's the average kind of time it takes?

Husayn: So from our side, as technology goes, if there are no issues with the ID or the selfie match, then it is typically sub 20 seconds so less than 20 seconds. If there is something that needs to be double checked, the average is two minutes so that's when a fraud expert for instance needs to double check something, the average return is two minutes.

Peter: So in those situations you've got a human standing by going through this in a manual process, is that correct?

Husayn: Correct, so hundreds of fraud experts when they need to double check something, but this is the time it takes on our side. You have to remember that, depending on the business, they have additional checks, additional processes…

Peter: Sure.

Husayn: Sometimes it might take up to 24 hours before reaching a conclusion, but in other use cases if it's a home sharing platform or if it is a travel platform then you kind of want to know within 30 or 40 seconds. So speed matters a lot specifically in those examples.

Peter: Right, right. Okay, so you mentioned machine learning a couple of times already, I think, can you explain...is the machine learning really in the recognition of the face itself? How are you using the technology?

Husayn: So in a number of ways, neural networks in particular, it is at different layers. So one is the classification of the documents so is it a passport, is it a driving license is it...for example, a California driving license and so on. Second is extraction of the characters; third is determining a range of different fraudulent patterns; font, style, it can be image tampering, it could be copy/paste and so on and so forth, but when we release a new model then as the results come through, we typically have to have humans double checking to annotate and correct, for instance, and that is what trains it. So it's human-assisted machine learning, especially for the fraudulent patterns or fraudulent factors.

And then there are the examples, as we talked previously about, the very sophisticated fakes that if they happen to be able to cheat our system then our client, two weeks or four weeks later, when someone hasn't paid their credit card or whatever it may be will flag to us that, for instance, this fake has cheated our system.

What they like the most is we use those samples to build the next version so that you can essentially fool us once, but it's going to be increasingly hard for you to fool us again. What businesses, in particular, care about is those sophisticated fakes. That is our pace of innovation and pace of improvement that really has helped set us apart and we've only been able to achieve that fundamentally as a result of our machine learning approach.

Peter: That's interesting. So you've got humans that are really helping the model improve and then is the model improving by itself anyway as well?

Husayn: So there are different models for different functions…when it comes to where human assistance is particularly useful is on the fraud factors and so when an ID comes through, if it needs to be double checked or if their thresholds haven't been met, humans are double checking and we have internal feedback loops.

Those internal feedback loops with our own team help significantly improve accuracy on the models because they are kind of eliminating the false positives and then we have external feedback loops with clients. Where again if we happen to have missed a sophisticated fake, they then flag it to us and then we use those samples to build future versions. So when it comes to what sets us apart which is fundamentally our fraud detection capabilities being so strong, that is the result of, in large parts, feedback loops both internally with our fraud experts, but also externally with clients.

Peter: Interesting, interesting. It seems like it's a bit of an arms race in some ways, or is it? Maybe you can answer that question because the fraudsters have access to the latest technology as well and they can hire people who are really smart as well, so do you find it an arms race, or do you feel like they won't go to your clients, they might go to somebody else who has less sophisticated type of, you know, type of fraud detection?

Husayn: Yeah, it is actually an arms race, but it is one that we are now able to effectively sort of counter. So in some ways, before us, the way I look at it is like they were armed with tanks and the solutions offered were knives at best because you don't need to be a sophisticated fraudster to just guess or steal someone's date of birth, name and address to be able to cheat and open an account.

But now, you have to show an ID and show your face and you have to make sure that all the fake techniques that capture all the attack vectors are prevented and so on and so forth. So what fraudsters, what they want to do the most is the sophisticated fraudsters want to commit fraud at scale so they want to cheat hundreds or impersonate a hundred people every day, for instance, and they are extremely sophisticated so they have…you can you imagine the super sophisticated ones often work out of office blocks, they have performance related pay, sick pay and everything else, very sophisticated machinery, very sophisticated techniques. But what they want to do more than anything else is actually to be able to cheat systems at scale, as I mentioned.

So what we do, especially with clients that you use our liveness check for instance, is you have to do a 10-second recording, you know, read three randomly generated numbers and do a task and so on. Now that isn't very scalable, first of all, you can't cheat that by doing or pretending to be someone else or holding up a photo, or something similar because it’s a challenge and it’s been designed to prevent that, for instance, and secondly, as a bad actor looking to cheat a platform, why would you go through one that is A. very time consuming and B. super difficult to cheat as opposed to many other alternatives that are much easier to cheat.

That's in many ways, why we've become the platform sitting behind a lot of the fintech community. All the communities are going online, including some of the mainstream banks. That's because by us sitting in the middle of all these different businesses, our models are learning from all the data and all the attack vectors that are sort of looking to be broken across all these different businesses. All models get stronger and all clients benefit as a result of a bad actor trying to cheat one system and therefore, we learn that pattern. So if that bad actor has sold a hundred fake IDs, we would catch the other 99 coming through other clients' for instance.

Peter: Right, right. When you're going into banks today, are you…this might be their first facial recognition or any kind of thing...it wasn't very long ago, you would open up a bank account or you even get a bank loan and there was nothing automated at the bank, it was all a manual process, so are you going into banks and this is their first foray into your kind of product and you're sort of starting from scratch, or are you going in and replacing what's existing?

Husayn: It’s a good question, in many ways both. So three or four years ago, the mainstream banks would talk to us, but we didn't feel as though they took the wave of the neo online challenger banks too seriously.

Peter: Right.

Husayn: In some ways some of the early assumptions were, you know, this is a new wave, it's a bit of a fad and how can you have a purely online bank. Surely, you’re going to get all the fraudsters disproportionately and therefore the model is going to crack or break. What everyone has been able to witness, especially in the last two or three years, is that these online banks not only have they been able to prove that they're scalable in on-boarding very many customers very rapidly, but more importantly, they don't have any excessive or any out of the norm fraud exposure than the mainstream banks.

So when these mainstream banks looked under the hood and saw that technology such as us in identity verification or (inaudible) for behavioral stuff or iovation or I guess, ComplyAdvantage for watchlist searches and different types of machine technologies being put together, assembled to help with the on-boarding compliance process, they've started to adopt since. And to your question as to whether is it new for them or not, what the mainstream banks are now doing and have been doing for a few years now is either they are buying an online bank or spinning up a completely different online bank division and for that it has been designed to be sort of new age and tech.

Once that model is proven out, it is reverted back to the bank. So if most of the mainstream banks...their tech stack is not necessarily equipped to be able to do work in an agile way, the way you'd expect a fintech or a neo bank would, but they are all moving in that direction and that's why we are partner with the Salesforce Financial Services Cloud, or equally BBVA might be one of the exceptions where as a bank it is public knowledge that their whole tech stack has been improved end-to-end to ensure that they're able to plug in the latest technology, specifically if it’s machine learning and API-based.

Peter: Right, right, okay, fair enough. So I'm curious about the fact that...you know, you're based in San Francisco, but your company is based in London. Tell us a little bit about where do you operate and why are you here and not in London, tell us a little bit about the structure of your company.

Husayn: Yeah of course. So, we're 240 people, the growth in sales in our largest market, our fastest growing market is in the US, hence, why I'm based here, but our engineering base and the technology side is predominantly in London, but also we have a team in Lisbon as well. So we have 7 offices in total, we have three or so colleagues in Paris, three in Delhi and also two in Singapore.

To your question of why I'm based in the States in particular, in large part because in Europe or at least western Europe, we are pretty much the leading provider in many ways. In the US, we are known in the community, but not as well known as we will be hopefully over the coming years so that's essentially why I’m here. As you can imagine, it's in many ways, a much larger market too.

Peter: Right, right, okay, fair enough. So I was reading recently about this Global Financial Innovation Network, GFIN, that cross border regulatory sandbox initiative. The FCA in the UK was one of the real driving forces behind this because this is a global problem that obviously knows no borders. I mean, the people hacking into these systems could be in Russia, they could be India, they could be in, you know, in Chile, we have no idea where these people are.

I'm curious about the fact that you've got all these different countries, there's certain best practices with fraud so maybe, with anti-fraud, I should say, so from a regulatory perspective how important is it for an initiative like this to kind of come together and really combat fraud in a global way?

Husayn: There is a big need and the regulators can play a big role so we've been very fortunate in that, having the majority of our product and technology team based in London with the Financial Conduct Authority and their sandbox approach and how they have both competition and innovation as their focus area. They've been able to help us and companies in a similar space as us work hard to get the right balance between using the latest technologies and achieving really strong outcomes and results. So we were part of the first FCA sandbox, for instance, and it was sort of announced a few weeks ago we're part of the current batch again so cohort 5.

With GFIN, GFIN is essentially, like you said, a similar setup to the FCA sandbox, but it's across multiple jurisdictions so we're part of the current GFIN batch too. It's the first time it's being done. So we're continuously communicating and engaged with the regulators because we want to help as many countries as possible enable an online digital ecosystem, but underpinned by strong fraud prevention techniques because more and more countries, not necessarily emerging, even to develops like BaFin, for instance, in Berlin and in Germany. They're looking at London and they're looking at Paris and New York and they can see the progress that fintechs have made that has been far more than what they've been able to achieve.

Peter: Right.

Husayn: One of the underlying reasons which is in Germany the regulation is still a little bit outdated, it requires like a video Skype call for instance for you to be able to sign up to a fintech whereas digital technologies can be used in most other jurisdictions. So we're continuously engaging and developing both learning and teaching, or sharing at least, and these sandboxes are the perfect forum to help facilitate that because the regulators are very much interested and very much want to learn, again, not just across the range of..not just the fintechs, but the platforms that are enablers to these fintechs.

Peter: Right, right, okay, makes sense. So I'd love to get your perspective on something. It's an issued that I've been thinking about for a long time...you know, obviously the Equifax hack a couple of years now and the whole idea of having your identity or details about your identity stored in a central database is...it already seems old fashioned, but we haven't really yet come up with a better way to store this data. How would you recommend we store identity data?

Husayn: So the first is to recognize how important and how sensitive it is and secondly, as you mentioned, it's how it currently operates which is not fit for purpose. So essentially, for the current model it's predominantly centered around credit bureaus' centralized leaking database. The antithesis or the solution or the counter to that would be the opposite which is a much more decentralized solution where the consumers own and control their legal identity.

So there are different models and we are partners to quite a few of the different technology solutions looking to solve this identity problem essentially calling it a portable identity or decentralized identity. Some are using blockchain, others are not, so different approaches, there is a wave of activity now that has been initiated and that is making progress.

The fundamental objectives are first of all, for the user to own and control their legal identity and share that with the businesses that they choose to so the actual way that’s stored. There are different models and different options, again, the consumer could choose. One would be your smartphone, for instance, in a secure way, an alternative would be your local bank or the bank that you trust with your finances. They could be a custodian of your legal identity, a third could be AWS, Azure or a cloud service, for instance.

So there are a number of ways and naturally, if it's in one place, you control and you are able to manage, it's going to be far superior and far more secure than what we have currently. What we have currently is you want to sign up to your local gym, you want to sign up to supermarket’s loyalty program or anything, any account that you want to open, you have to share so much data.

That exponentially increases the likelihood of one of those businesses getting breached and therefore your data leaking on the dark web and therefore, bad actors being able to very easily use that data to open accounts in your name. So we have no doubt that the future is going to be much more of a decentralized trust and a network in the sense of portable identity and because we believe in it, we're actually very involved in helping different platforms looking to solve that problem.

Peter: Right, right. So we're almost out of time, but a couple of things I want to get to. You know, I think about this, do you think that in the future, in the distant future, do you feel like identity theft is going to be just a solved problem where it'll be so rare as to be very unusual because tools like yours get so sophisticated, or do you think we're always going to be challenged by this?

Husayn: I think that there will be...I can’t say it can’t get worse because it’s actually getting worse, (Peter laughs) but there is now effective technology out there to address it. So it's going to be...you're probably going to see two camps; those who are deploying effective technology and therefore are able to be protected and those who are not which increasingly are going to find it difficult, both costly and so on, to continue. This is ripe for there to be a network of trust built that gets stronger, the more data there is and therefore is able to offer all the benefits because of different drivers there is increasing regulation around privacy and around security, there is consumer demand for personalization and efficiency.

There is a growing...I guess, the power of machine learning only in the last five/six years has really been able to show itself and all the benefits that it brings and so on and so forth. So the answer to your question is that we are going to very much solve this identity problem, but it's going to take some time, but we're definitely on the right path.

Peter: Right, right. Okay, last question then, what are you working on right now, what are some of the things that you're excited about that might be coming down the track?

Husayn: So in some ways, I'm kind of interested anything with similar use cases, or interesting patterns in different geographies. So one of the companies I am following closely…one of our partners is Tala, for instance, in emerging markets like the Philippines, Indonesia and elsewhere, they're able to do micro loans so $20, $50 lending and they are able to do so because it's all online and they've been able to reduce the on-boarding cost to a few dollars as opposed to tens of dollars if they were required to see everyone face-to-face.

On the other end of the world you have...if you look at Southeast Asia, examples of MoneyMatch or similar ones that are doing very, very cool stuff. So across the board the fintech wave in many ways is still the first wave and it's catching on in different parts of the world so it's very interesting and exciting to see that.

Secondly, back here in the States it is, and sort of the UK, we're running some pilots on portable identity so the topic we were just discussing. Ultimately, it's going to be the user that owns and controls their legal identity and they're able to decide which businesses they want to take that to so that's going to be pretty exciting to see it progress.

Peter: Okay, yes, it's going to be fascinating to see it. I find this whole topic just so interesting that we are here in this process of moving to a completely different way of doing things. Anyway, Husayn, we'll have to leave it there. I very much appreciate you coming on the show today.

Husayn: Likewise, thank you for the time.

Peter: Okay, see you.

Husayn: Bye for now.

Peter: You know I was reflecting on this after I hung up the phone with Husayn and, you know, I've recently opened up a couple of new accounts, I'm not going to name names, but sometimes the systems to open these accounts even with fintech players, they're not as sophisticated as I expect, particularly when it comes to identity verification. I'm sometimes now expecting to have a video or sophisticated photo verification done with ID and oftentimes, that's not the case.

I think in Europe it's probably more so, but here in the US I think we still have a long way to go before we get an identity verification system that everybody uses and I think companies like Onfido are really going to help drive this change where they have the easy to use systems that catch so much when it comes to the bad actors.

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

Today's show was sponsored by LendIt Fintech Europe 2019, Europe's leading event for innovation and financial services. It's happening September 26th and 27th at the Business Design Centre in London. Registration is now open as well as speaker applications. Find out more by going to lendit.com/europe

(closing music)