LEND ACADEMY

PODCAST TRANSCRIPTION SESSION NO. 92: FRANK TERUEL

Welcome to the Lend Academy Podcast. Episode No. 92. This is your host, Peter Renton, Founder of Lend Academy.

(music)

Peter Renton: Today on the show, we are talking digital identity and fraud prevention. I'm delighted to welcome Frank Terrell. He is the CFO of ThreatMetrix. Now ThreatMetrix have been around for a while and they are one of the leaders in this online fraud prevention space. I really didn't have much idea how this all works, but after this interview, I now know a lot more. It really is fascinating, the work they're doing, and how they can take data points from different places and be able to really understand who is that person that is typing in a loan application in front of their computer or on their mobile phone, or what have you. They have such sophisticated systems and we go into that in some depth, we talk about the professional criminals, what they're doing, we go into the mechanics behind how they are able to detect fraud. We talk about different countries they're in and what they have planned for the future. It was a fascinating interview, hope you enjoy the show!

Welcome to the podcast, Frank.

Frank Terrell: Thank you, Peter, pleasure to be here.

Peter: So let's get started. I want to give the listeners a little bit of background about yourself, particularly about your career before you joined ThreatMetrix.

Frank: So thanks for that, Peter. I've been a tech guy here in the Valley since the early 90s and most of that time focused on software or much of that time and certainly much of that time focused on security, authentication, access control, those kind of things. I had the opportunity to be privileged to work with some great management teams, this is one of them; second time the CEO and I have done a gig together and really excited to be part of this team.

Peter: Okay, so then tell me about how you came to work for ThreatMetrix.

Frank: So it's interesting, ThreatMetrix...I'll give you a little bit of the history of the company and kind of rope in my arrival here. So ThreatMetrix started off as a company focused on really understanding how people interacted with websites and by that I mean to really get a deep analysis and understanding of the device. You know, when someone comes to a website on the other end of a transaction, it's important to know...is that interaction compromised because they are accessing that website through some device that's inherently compromisable.

So the company's early days were focused on understanding things like if someone was behind a proxy, what the true IP was, if in fact the machine was compromised, was there malware on the machine, is there something wrong with it, was the machine acting in some anomalous fashion or was there something about the machine that was counter intuitive. For example, am I

interacting with a US website, but I've got no English fonts on the machine, those kinds of things.

What intrigued me was that the amount of interaction that ThreatMetrix was having with its install basis, its customers and the growth of that customer base really lent itself to the reality that ThreatMetrix was going to develop in short order, one of the largest private networks holding information on consumers globally that could be used to prevent fraud and to reduce friction on good customers so that intrigued me. As I said, Reed Taussig, our CEO and I had done another deal together a few years back and so Reed and I connected and I joined the company a little over five years ago.

Peter: Okay, so what do you do there exactly?

Frank: So I'm the Chief Financial Officer so I have the privilege of running obviously the financial side of the shop, but also interacting with many of our customers, you know, really understanding their needs, working with them as we negotiate our deals. And so it's really a broad and really good role; a chance to really get deep in the weeds, if you will, on the types of customers we have, the challenges they face and how we help mitigate and solve those challenges.

Peter: Okay, so let's just talk about that a little bit. Who are the typical customers that you have and how are they using your products and services?

Frank: So ThreatMetrix, in a nutshell Peter, really helps customers authenticate who is on the other end of a transaction and we do that by focusing on identifying people's online personas. If you think of the world we live in today and the best way to get a picture of this is open up your iPhone or your Android device, your smartphone and look at the number of e-mail addresses that you actively track on that device. Each of those e-mail addresses have a different purpose, a different reason you're tracking them and really functions as a separate online persona.

In the physical world, in the real world, you and I have just met over the phone and I'm Frank, you're Peter and what we know about each other is what we exchange with each other, but in the online world, you know, I can have multiple personas. I can have an e-mail address associated with spam protections so whenever I'm surfing the internet and signing up for stuff and I don't want my inbox buried at work, I have a spam account.

I've got an account with my alma mater, my kids are all grown and through college, and so I've got e-mail accounts associated with their schools, I've got my ThreatMetrix account, I'm here in Santa Clara in the MBA program so I've got a Santa Clara account; every one of those accounts operates and functions on the internet as an individual persona. What ThreatMetrix does is it takes those individual's personas and stitches them together into one digital identity and the premise being that it's impossible to authenticate Frank unless I can look at all of his disparate personas online and make sure that none of them has been compromised.

So think of it this way, we take how you interact with a website, that's the device piece then we do deep device analytics and really get deep on...you know, if there's any compromisable situation or something wrong with the device. We marry that device information with the one digital identity that's an amalgam of your digital personas and then what we do is we understand how that group is behaving in real time in our global network.

So if I could understand who you are holistically, how you're behaving and how you're interacting with me, I've got a far better way of authenticating you and deciding whether or not to trust you or not. That's what we provide our customers, we provide the ability for them to say okay, this individual appears to be operating in a non-anomalous fashion and we can trust this individual or this individual is doing something that clearly is weird and we're not going to trust them. We provide that intelligence feed to our customers.

Peter: That's fascinating. I actually want to dig in a little bit here because I think it's something that I don't think a lot of people know about. I know I don't really know about what happens when you're on a website and you might be putting in your credit card information, you might be trying to obtain a loan.

So, you know, I'm basically...just an example, with a marketplace lending site, so you go to Lending Club, you give them like eight pieces of information that is…you're not even giving them your Social Security number, you're just giving them your e-mail, you give them your name, and your address, and that sort of thing...so there is this eight pieces of information and then you're coming in between…when you click Enter and then you go on to the next screen and it all happens in like a second...so you're basically taking the information that I've entered and you are determining whether or not I am who I say I am based on that eight pieces of information.

Can you just tell us a little bit…obviously don't give away your secret sauce, but how do you do that?

Frank: Yeah, it's a great question, Peter. Think of it this way and by the way, e-lending, peer to peer lending, fintech, in general, is a very large space for us. To put it in perspective, just in 2016, our estimate is that we prevented a billion dollars in loan origination fraud by protecting over a million new account or new loans, signatures through our various e-lenders so we know this space well, but think of that model, I mean, it's a very difficult problem that fintech is facing.

You're a lending company, you're a peer to peer lender and, you know, you've already got the inherent credit risk built in any transaction, you know, is this person ever going to service this loan and pay it back so that's a given. What's new in fintech and what's new for e-lenders is, you know, I don't know who Peter is; I'm relying simply on information and you may be somebody with a thin file so you haven't got a lot of a legacy authentication methods, there's not a lot in the credit bureaus about you and so they're having to rely and make a split second decision on whether or not to give you a loan. If they give you the loan and you're not Peter then that money

is gone, never to be seen again and if they don't give you a loan and you are Peter then you're aggravated and you take your business to a competitor.

On the one hand you've got fraud, and the loan walks away; on the other hand, I've got an aggravated customer who takes marketshare to my competitor, both of which are bad. So what we do is we allow our e-lenders to use our portal and our rules engine to write the rules that matter to them and they might say, you know, I'm interested in creating rules that are geographically balanced. So they might say, look, if Peter is more than 50 miles from home and applying for a loan, we're going to reject Peter because people normally don't travel to apply for loans, right?

Or, they might say, if Peter has applied for a loan, if this persona has applied for a loan anywhere else in your global network in the last 24 hours then we're not going to allow him to apply for a loan because he could be stacking, he could be applying for loans at ten different places and not really be Peter.

Now here's the beauty of the ThreatMetrix offering, we have a privacy by design feature that basically says, I'm able to provide these individuals relevant transactional information, relevant persona information and relevant device information and I'm able to give it to them without ever compromising PII. Our standard tagline here at the company is, I don't need to know your name to know who you are. I know who you are based on the corollaries and conclusions that we make on this anonymized data that our customers send us and then we feed them back the answers to the assertions they've made against our network.

So in the prior example, the lending institution might say, okay, is Peter in fact, more than 50 miles from home and has this individual applied for a loan anywhere else in your global network in the last 24 hours. If the answer to both of those is yes, that may trigger, in their mind, too much of a risk to allow the loan to proceed. So we provide them that information and the reason we're able to do it, and this is really one of the great differentiators of our company, is that we run somewhere around 2 billion billable transactions a month across almost 5,000 customers and that customer group is broken up between financial institutions, e-commerce, media, government and insurance. And so we're basically covering almost the entire gamut of the industries in which people would traffic and people would transact with.

By doing that and by having our technology that always follows data elements around and provides the same identifier every time we see them, we're able to say that, in fact, somebody with a credential that was just sent to us by the lending institution has in fact applied for another loan somewhere else in our global network. We're able to provide that information back to that lending institution without telling them who the individual was or where they applied for the loan simply that that did in fact happen and if that's important in their risk assessment then they would say, great, we're not going to approve this loan.

You hit on this earlier, Peter, everything I just told you happens in somewhere around a hundred milliseconds so in the time it takes you to hit Submit, we've gone through this analysis of your

digital identity and how it's behaving online and how you're interacting with the site and feed back the information that our customers assert against the network so they can make a decision as to whether or not to allow you to proceed or whether or not to review or to cancel that transaction.

Peter: It sounds like you're doing a couple of things there. You're looking at your own internal database that you have basically collected information on with your customers, whether it be e-commerce transactions, insurance applications, loan applications, whatever, so obviously you've got a very rich internal database so I guess there's that piece. The other piece is...you said it a couple of times, you said how they're interacting with the computer like...so tell us a little bit how those two pieces interplay.

Frank: Sure, at a very basic element, you know, is it really a device. I mean, does it have the attributes of a device, or is this a botnet. I mean we're able to differentiate whether or not this is a real interaction or whether it's a fake interaction. What kind of device is it, is it mobile, is it a tablet, is it a PC or Mac. If it's a mobile, obviously, or a tablet they're using an app, then we're built into the SDKs and that gives us very rich information about that interaction. Is there malware on the device, is there somebody trying to inject something into that session?

So we have a lot of information on that side of it that's important, but then equally importantly, you know, what about the persona associated with this device? So has Peter's e-mail address and this device been associated with any weird element? For example, we may be able to tell you that your e-mail address is now being used on 27 different devices across four different continents and three different time zones and obviously, that's an indication that you've been compromised.

Peter: Right.

Frank: Peter, the way we're able to do this...I mean, just to give you a glimpse into the breadth of the ThreatMetrix digital identity network. Today, we're tracking over 4.5 billion connected devices online. We know something about 1.5 billion people online. If you consider that in the world today, you know, 3 billion people are actively involved in commerce on the internet, that says that we know something about 50% of them.

As I said, we process over 2 billion transactions a month, we're tracking almost a billion IP addresses, we've got coverage in over 200 countries, almost a billion e-mail addresses that are in our network. We stop somewhere around 600 to 700 million attacks every year globally against our customers and we're tracking somewhere north of 700 million physical ship to addresses which is also an important attribute. You would like to know that if you're buying something on an e-commerce site that that device and credential combination is not at the same time associated with 13 known bad ship to addresses.

Peter: Right.

Frank: So the global network gives us the ability, because of its coverage and its breadth, to really understand as an anonymous device and credential combination are presented to us and then our customers make assertions against our network on things that matter to them or risks that matter to them, we're able to provide them very quickly salient information, and say, yes in fact we think this is compromised or not compromised or more importantly, this is Peter.

Interestingly, Peter, if you look at the reason people buy our stuff, over 50% of people that come to ThreatMetrix are coming to us because there's too much friction in the channel. Somebody in high tier operations has freaked out because of fraud or whatever and has made it so difficult to transact with us or with the customer that they need help. What's happening is customers are abandoning transactions and going elsewhere.

As we started the conversation, think about it, if you can't get a loan at one lender, you're going to go to the next one and what's happening is that lender is losing the top line benefit of real revenue because you turn out to be a legitimate customer. So over 50% of our customers buy to reduce friction.

The benefit of reducing friction is one, I get more revenue; two, I reduce operational costs associated with step-ups and challenges and then also the other reason they buy is to prevent bad guys or bad actors from transacting. That was the billion dollar number I gave you. Last year, in 2016, just in our e-lending vertical, we estimated it's about a billion dollars in loan originations that we protected from fraudulent originations and that's a pretty significant number just for that group of folks.

Peter: Right, right. So let's just talk about the bad actors for a second. Obviously, there are those people who have just given up and their credit is about to be trashed so they're going to try and get some money in before they can't do it anymore. So there's those people, but then there's also the professional criminal who is trying to look for ways to basically game the system to try and obtain money. Obviously, online lenders have got to be a target for these kinds of people, so can you tell us about…are professional criminals attacking this space, how are they doing it and how are you stopping them?

Frank: Yeah, I mean, it's a great question and the answer may surprise you. In fact, there's a number of different antagonists that we see across the industry, so think of the e-lending vertical so, you just said it.

There's two things going on. Number one, by going to the dark web and spending a little bit of time surfing around, you're very quickly able to get information on how to do this stuff. A lot of the folks that are out there trying this stuff are really less sophisticated than you think. There are folks that have developed a reputation on the dark web, that have downloaded some tools to help them interactively try to compromise stuff.

The other antagonists are, as you said, organized crime, professional criminals, states who are antagonistic to our own interests, who are trying to be disruptive economically and obviously, those folks are much more sophisticated. But think of this, I mean, if you're the merchant, in this

case you're the lender and you're let's say competing in a market of 50 other lenders, you know, absent of networks like ThreatMetrix that is providing global shared intelligence across that entire group of folks...how are you going to know if Peter has applied for 15 loans at exactly the same time on 15 different devices at 15 different websites?

What happens is where there's been sophistication is in the vectors, the attack vectors are very interesting. So you got these professionals that say, hey look, I understand that in many cases there are thin files and in many cases the loan value is small enough where the lender is willing to take much more risk than say a bank would and so I'm going to apply for ten $5,000 loans at once. I'm going to do it at ten different e-lenders and I'm probably going to get accepted at five of them and I'm going to walk out of here with $25,000 that I otherwise wouldn't have had.

So unless you have a network where one of our customers could say, as I said earlier, hey, has Peter applied for a loan anywhere in the last 24 hours in your network, unless I can tell them that and say, yes, in fact this individual, as a persona has applied for a network, they're not going to know if they're at risk or not. So, yes, the antagonists are sophisticated, they're well prepared...what's very interesting about the group of folks that they...you know, they're not just good at the fraud and the ways to attack, they're also very good domain experts in certain industries.

By that I mean they know how loan originations work, they know how payments or transfers work. And so you're dealing with both the aspiring new bad guy who goes to the dark web and gets some tools and is able to compromise less sophisticated infrastructure and sites and you're also dealing with very professional folks that are either organized crime or, as I said, antagonistic states that understand how these things work and are able to en masse, really perpetrate significant amounts of fraud at once because these companies have no way of identifying whether or not these folks are legitimate.

Again, the benefit of ThreatMetrix is everything we do is anonymized, all those ten vendors that are all lending at the same time never really get your name. They don't know that it's you as an individual, but they know that this persistent data element is applying for loans across our network, they don't know where they're applying which preserves the confidentiality of each vendor, but they do know that there's a risk because it's highly unlikely that one individual is going to apply for ten loans at the same time across ten different devices and ten different organizations.

So the benefit of ThreatMetrix is that we provide our customers global shared intelligence derived from this very large digital identity network that is, think of it this way, it's being refreshed roughly 80 million times a day. You know, 80 million transactions a day, that network is being refreshed with more and more information as it relates to your digital identity. It's being done so anonymously so you're never ever in a position where your PII's compromised, you're never going to run into regulatory hot waters or headwinds, but at the same time I'm able to provide those lenders with information that's invaluable to them.

I mean, think about it, if those five lenders would say, you know what, this guy is applying for more than one loan, I'm out. That decision to not proceed with the transaction probably just saved them $5,000. So it's kind of where the future is going. In a digital first world where everybody's rushing to mobile, everybody's rushing to get their businesses online, especially in e-lending and peer to peer lending, in fintech, in general, in that world where there's kind of a race to finish line, you need to have global shared intelligence from a reliable source that can give you accurate salient information as to whether or not to proceed because, quite frankly, as I said early on, you may be a legitimate customer with a thin file, but still a legitimate customer in which case they should give you the loan. Or, you could be a bad guy pretending to be Peter in which case they shouldn't give you the loan and the ability to make that decision in real time is instrumental into your business.

So we provide them that ability, and as I said, we do it over 2 billion times a month. Put that in perspective, what that translates into, and this is a really interesting statistic, if you look globally at our recognition rate, you know, on average across the globe, 95% of the time when somebody lands on a website we protect, whether that's through a PC, a mobile or a tablet, when they land on that website we know something about them somewhere else in our global network. So you're talking about a massive global footprint that allows us to have this anonymous global shared intelligence that benefits our customers in terms of, as I said, taking on revenue when they should, reducing operational costs associated with step-ups and at the same time preventing fraud.

Peter: Yeah, it's fascinating, fascinating because I know...I think I read somewhere that you've got some large Chinese customers. You know, that's obviously a country where there's a massive number of thin file people who are slowly entering the middle class. So what are some of the differences then?

I love the fact that you've got this global network, that you can sort of detect what people are doing, things in different countries, but you also...you must have this massive amount of intelligence about different countries themselves. It was interesting, I had Jeff Stewart from Lenddo on just last week and we were talking a bit about this. So what do you notice about the differences between countries like what is the difference between a Chinese consumer and an American consumer? Are they just as easy to identify when it comes to fraud or are there different challenges?

Frank: Yeah, it's a great question, Peter. One of the benefits of having a global network is that we're able to identify good customers. I mean, one of my initial premises was, look, at the end of the day, the number one reason that people buy us or the reason they come to ThreatMetrix is they want to reduce friction because they're letting good customers kind of fall through the cracks.

Imagine the Chinese customer scenario; you know, I am a businessman in Shanghai, I decide to come to San Francisco, I want to rent a hotel room in San Francisco and I use my Chinese credit card. Regretfully, most of the time, unless you've got the benefit of a global shared

network, that transaction is probably rejected because that's a Chinese credit card and people don't know how to authenticate it.

Now imagine I'm a Chinese business person and as you said, I'm in Shanghai somewhere, I'm a young entrepreneur and I want to get a loan and I just recently moved in to my apartment in Shanghai, I've got, think of the legacy authenticators. I don't have a home phone which is a big part of the normal credit bureau process, I haven't been in my address more than five years so I appear to be transient, I don't have a job per se because I'm an entrepreneur and I'm bootstrapping a business. I mean, all of those things that are traditional anchors in a credit file by a credit bureau aren't going to exist for you and yet you might be a legitimate business guy trying to get a loan in Shanghai. The only thing you can rely on then is to understand...to be able to vet this customer and say, look, this is individual, we know this individual, again, anonymously, but we know this individual, this digital persona, we know that it operates, we know that it's been authenticated elsewhere in our network positively that people have either stepped it up or they've legitimately authenticated this transaction and this person so we're going to rely on that global shared intelligence to say this appears to be the right individual, the device isn't compromised, there's nothing anomalous about the interaction other than there's no history in the traditional sense. So in that sense, the Chinese and American consumer are exactly the same because we don't have to rely on, in a digital first world, on traditional authentication methodologies which, quite frankly are outdated and even if you did have it are going to give you false positives.

Peter: Right.

Frank: If you went to one of the credit bureaus in China and you said, alright, this guy's applying for a loan, the response you'd probably get back is, no home phone number, been at the address less than a year and no known job and you're probably not going to get the loan and yet that individual may be somebody who is a very good consumer and a very good customer and conducting business.

So the differentiation and distinction globally is that in a world where everybody online is global and you are today, the reality is if you're online, if you're selling anything online, you're a global business, why should you limit yourself to certain domestic customers and walk away from international revenue, especially when statistically 70% of those people that are trying to interact internationally are legitimate customers.

And what we provide our customers is the confidence to be able to say, yeah, this appears to be...again, based on what matters to them, based on the rules and risks that matter to them and within the portal when they write these rules to say, yeah, based on the criteria you've established, this appears to be a legitimate customer, I'm going to go ahead and transact with them because I know that in this particular case the Chinese businessman who's about to apply for a loan was authenticated at a global bank, logged into his account, was authenticated as a real individual or we know this individual has been authenticated at large e-commerce sites and

can be trusted. I think that interplay between not just the individual and the geography, but also everything that individual does is super critical.

One of the interesting things that I think people miss in this global shared intelligence world and one of the great differentiators for us is that oftentimes you'll have these people that want to establish consortiums and they'll say, look, why don't we share information amongst ourselves as it relates to banking, for example. And so someone comes to your bank and this individual is a good customer then we'll let everybody know they are a good customer.

The beauty of having a diverse network is people that bank also buy e-commerce stuff and people that buy e-commerce stuff also watch movies online and people that watch movies online also buy insurance or apply for visas on government websites. So when you've got a broad view of how an individual behaves across the various sectors, you have much more powerful information about transaction authenticity, if you will, because you're watching this individual interact across a number of different industries in ways that are either consistent, consistently inconsistent or just wrong and we're able to provide that information.

Peter: So how do you...I mean, you've got this massive data and so on every individual you must have thousands sometimes, I imagine tens of thousands of data points and I can imagine that there would be some privacy people who aren't too happy about how much data you have. How do you answer those concerns?

Frank: Yeah and again, the beauty of the privacy by design feature is that we never ever, ever traffic in personal information, I mean, there is no PII that we traffic in. Just to put the technical phrase on it or terms but when we get information it's immediately anonymized with a one way hash so it can't be de-anonymized and that one way hash is persistent in our networks.

So when a data element shows up, we know that we've seen that data element before. I don't know that it's peter@gmail, I just know that that data element and that identifier is persistent and every time that data element shows up somewhere else, I can identify it. So I can tell my customers, you know, very, very accurate information about anonymized personas without ever knowing their name or ever compromising any PII.

So that's given us the benefit of being the largest player in e-commerce in our space, of having a huge traction with global banks. You know, we've had a fantastic year in 2017 with global financial institutions, with government, with media. All of them are comfortable that one, I am not violating regulatory concerns because everything we do is based on anonymous corollaries and conclusions; number two, I'm ensuring the results of those corollaries and conclusions with the other customers, not the underlying data elements, because I can't because, again, they're just anonymized information.

And so the combination of those two things allows us to very quickly onboard customers in this space irrespective of those regulatory concerns and get them up and running without ever compromising PII and that's a huge differentiator.

Peter: Right.

Frank: We know things about numbers of people. You know, I can tell you for example that we're tracking 1.5 or 1.4 billion people on the internet, I don't know their names. I don't know who they are, I don't know anything about them personally, but I know how they transact, I know how they act online, I know how their anonymous digital identity behaves and so we rely on that information to share with our customers.

Peter: So even then if someone was able to hack into your systems and get a copy of your database, what you're saying is it would be useless because they wouldn't actually have any data that they could use?

Frank: Right, and the other thing that's interesting, every customer has their own access to the data and their own encryption keys. We don't have them so only the customer is able to see their data so in the unlikely event that this were to ever happen, knock on wood, it never has and we hope it never will, it doesn't really matter because what you would get is just a bunch of information that can't be de-anonymized.

Peter: Okay, so I know that you recently raised $30 mIllion in debt financing from Silicon Valley Bank, I'm just curious about that and why did you do debt instead of equity?

Frank: It's a very good question. The benefit of ThreatMetrix now in its 10th year of operation is that the company runs a very tight business model. We're experiencing tremendous growth, over 50% year over year, we run the expense out of the business very tight and so the company is effectively cash generative every year, but we wanted to have a non-dilutive cushion, if you will, to allow us to make investments in other things.

So we have this facility, it has a lot of runway, if we need it we can use it, we haven't had to yet, but it really was a desire to say, we want to have some fuel if we need it to be able to invest in new channels, to continue our investment innovation over and above what our working capital provides. So the company is just doing fantastic, we have very strong margins and we're very, very proud of the business and the way it's run.

We figured that rather than raise equity and go through the process of having to go through valuations and the potential dilution associated with it…at Silicon Valley Bank, which, by the way, is a fantastic customer of ours, has been a great partner. Silicon Valley provided us with a facility at incredibly favorable terms that we just couldn't ignore.

Peter: Right, okay, so last question then. What are you working on right now, what can we expect coming out of ThreatMetrix in 2017?

Frank: You know, it's amazing, our Chief Products Officer and our CTO, Alisdair and Andreas have done a fantastic job in the product roadmap and the engineering associated with the company. If you think of our business today, we have a digital and threat intelligence platform that provides much of what we talked about then we have something called Dynamic

Decisioning Platform which allows you to make decisions and dynamically kind of make assessments of data as you go through. That allows you to do things like onboard other data through our integration/orchestration hubs, it provides machine learning and AI as it relates to smart analytics so that we can now write rules that teach themselves and these algorithms learn how these fraud vectors are happening.

You can imagine, Peter, that in a world where we're processing 80/90 million transactions a day, you need to have this incredible scalable technology to be able to identify those vectors quickly, provide ways to remediate them and feed those out to our customers. So we're looking at that, we've got a fantastic portal and case management suite that allows ThreatMetrix to be the system of record so that the practitioners of these accounts as they're working through these decisions are relying on us holistically for all of their data. So there's just a lot associated with proliferating the digital intelligence and a ThreatMetrix identity throughout the internet.

You know, if you think of our business, it grows about 100 customers a quarter, so that kind of growth. Every one of those customers brings additional new individuals. We anticipate that that 1.5 billion number of individuals we know something about on the internet will expand dramatically and what we're seeing is more and more of our customer relying on our ThreatMetrix technology to identify them, authenticate them and make a decision. So we'll see that proliferate and continue, we'll see the deployment of our Dynamic Decisioning platform so that you've got machine learning, smart analytics, decision management, plus this orchestration hub available to our customers.

The orchestration hub, by the way, is a great differentiator in this sense. We can now approach a customer and say, look, whatever other information you're using to make decisions, you don't have to replace that; we can coexist with it, we'll onboard that data, provide it an identifier and simply use it as another data element in our network. So what you have is a practitioner gets to say wow, I've made this legacy investment, there's no need to rip it out, I'm going to take that information and since we combine it with the ThreatMetrix global shared intelligence, so I can make better decisions relative to my customers.

So big year for us, a lot of fantastic technology, we have a super strong intellectual property portfolio, we'll continue to invest in that. We're going to see, again, good traction in APAC, a lot happening in our Asia Pacific business so, all in all, 2017 is a big year for us. I think we're going to see both on the product and business side some tremendous growth and, again, the proliferation of our ThreatMetrix identifiers into more and more customers across the globe.

Peter: Okay, it's fascinating, Frank, you really have an interesting business and certainly one that...digital identity is only going to become more important as we go forward. Anyway, I very much appreciate you coming on the show today, Frank.

Frank: Peter, I appreciate it, thanks for the time.

Peter: Okay, bye.

Frank: Bye.

Peter: You know, I was discussing with Frank after we turned the microphone off that digital identity really is a growth industry, it's something that is only going to become more important as more and more of our lives migrate online and we spend more time online and we have more interactions online. This is an industry that is critical for the success of any online endeavor, particularly the online lending space. So I feel like companies like ThreatMetrix are providing such a valuable service that without them there would be more fraud, investors wouldn't get as good of a return and we would really not have as much of a flourishing industry as we do.

Anyway, before I sign off, I just want to give people a reminder. If you haven't reviewed the show, we would love for you to go to iTunes and give us your honest review or Stitcher for that matter, we're available on both places. Give us an honest review, we'd love to hear it…I read every single review that we get and if you haven't done so and you have been listening to the show for a while, please, I ask you, go ahead and give us the review. It helps other people find the show and helps us grow our audience.

On that note, I'll sign off, thank you very much for listening and I'll catch you next time. Bye.

(closing music)