Albert Chow:

This is IT Visionaries, your number one source for actionable insights and exclusive interviews with CIOs, CTOs, and CISOs, and many more. I'm your host, Albert Chow, a former CIO, former sales VP, and now podcast host. Welcome everyone to another episode of IT Visionaries. And today we have a special guest. His name is Philip Dunkelberger and he is CEO of a company. And I love the name by the way. It is Nok Nok Labs, but it is spelled funny because all software companies got to spell something funny. It's N-O-K N-O-K, Nok Nok Labs. Philip, welcome to the show.

Philip Dunkelberger:

Hey, it's great to be here. Thank you.

Albert Chow:

All right. Nok Nok sounds like you're trying to tell me who's at the door. Why don't you tell our audience, what is Nok Nok Labs? What do you guys specialize in?

Philip Dunkelberger:

We specialize in authenticating the user and devices that are trying to get essentially services on the internet. We have done that and you caught the joke when I say knock, knock, what do you say back?

Albert Chow:

Who's there?

Philip Dunkelberger:

And that's what we've been trying to establish for like 30 years on the internet. Who is really at the end of the line? Is it a dog at the end of the line? Is it an imposter? Is it a hacker? We're set up to try to finish the idea and get rid of passwords and make it much easier, much more secure to log into your services.

Albert Chow:

All right, let's dive right in, because you're not the first and you won't be the last person trying to solve this problem. Arguably this problem has not been figured out since the early '90s, because the early '90s was the first time I was introduced to computers and there were passwords then and there are still passwords today. There are added layers of security trying to make us, like we just talked about before the show started recording, jump through some hoops to prove that I'm a person or I am who I say am. There's 2FA, there's all kinds of things going on. Give us an idea for our audience. What is Nok Nok Labs attempting to do that's maybe a little bit different than what the industry or some of the other players in the market are trying to accomplish?

Philip Dunkelberger:

Yeah, I think that the real key here is we needed, the design that we came up with was we were not trying to recreate all of the other things that have gone on, whether it's background heuristics, trying to figure out who you are, whether it's knowledge based authentication. What we were trying to do is say, let's look at this as a standard plug and play. Let's plug and play. Let's build a protocol that we put through the standards regime and make it work. And that thing became what is known as FIDO. Fast identity online. Many of your listeners are going to know about this thing that is being talked about called passkeys. Passkeys are built on this FIDO protocol. And essentially what the protocol was

designed to do is very easily say if you have an endpoint and you are a relying party and you want to secure that endpoint, usually in the past, to your point, these things have stopped at the device. Authentication goes to device level authentication, and then we got to try to figure out who the user is.

What FIDO did was say universally we will build authenticators that will show you who the user, the device, and the service they were enrolled in. So the beauty of this thing is it gives control back to relying parties, your bank, your e-commerce vendor, your medical vendor, and lets them enroll you, deploy public-private key pairs and that's what it's based on. It's no longer based on an on off or shared secret view of authentication. And that whole idea was can we build something better and make it a standard way working through industry standard bodies to make software both easier to use and secure in the area of authenticating a user?

Albert Chow:

All right, so for anyone who's listening to this show who's not maybe not familiar with what FIDO is, give us an idea of what's different. So I will use, for example, and I'm going to call them out right now, I'm going to use an example of a service I use that is really annoying and constantly makes me try to validate myself, although I'm happy they do it, and that's going to be Vanguard. I'm not bleeping that out. Vanguard, I'm calling you guys out.

So on the Vanguard mobile app, I have to log in user password combo. It always wants to send me a 2FA. No matter how many times I say remember this device, it just cannot do it. It cannot remember the device. And a lot of times also the 2FA, for whatever reason, it gets unsynced. It'll literally text me a 2FA code and I'll enter it in and they'll say it's not the right one. I'm like, I don't have another way to do this. So give us an idea, because you mentioned it's going to be user, it's device, and I think there's a third layer you mentioned. Talk me through how it should be.

Philip Dunkelberger:

What it should be is you log in your device and your device logs you into the service. And the way that that is created is fundamentally, instead of using on off shared secrets, a lot of things your audience remembers and is familiar with are using SMSOTP, which is of course is a shared secret one-time password that's time based. All of these things are layers on trying to fix the password problem. Okay? And then what happens is you have SMSOTP for instance has been broken for years. And in fact, last year, one of the big discussions at Money 2020 docking banking FinTech now is a vertical. They were saying, hey, these guys used to harvest maybe 10, 20 users an hour. They're harvesting SMS calls at 1,000 plus an hour.

Albert Chow:

What do you mean harvesting?

Philip Dunkelberger:

So you're there waiting for your SMS, okay, and it goes, they send it out, but somebody's intercepted your SMS. They're essentially mimicking your device. They intercept your SMS, they go in and now log in as you because they've already got your username and password. Now they have the SMS. And the back end goes, oh great, Albert, nice to see you. It's a hacker who changes the thing, moves money. And by the time you get that famous, hey, is somebody trying to log into your account it seems from another place? Is this you? You go, yeah, won't let me log in anymore because they went in and changed the

password, they went in and moved money, and now you're sitting there going, I didn't do any of that. And then the alarms go off that they've got a problem with somebody harvesting their SMS capability.

So these hacks are becoming very sophisticated. The same tools we keep talking about, they're going to protect everybody, AI machine learning, you don't think the hackers have those tools? You don't think the hackers have the ability to mimic your devices at scale? They do, because this is a multi-billion dollar business around the world. Now that kind of, for lack of a better term, FUD that keeps coming up. All the hacks and the cost of a data breach, that's all true. But the fact of the matter is, what we keep doing is piling more and more things on the user. Okay, like you said, SMSOTP. If it doesn't work, what do they tell you to do? Please call the contact center and you're going to notice things that you're having trouble logging in. Then you call the contact center and they take you through 14 more questions of who's your mother's maiden name, what was the last thing you bought online?

We see you're dialing in, you're going, yeah, I'm dialing in from the beach. I usually dial in from my home. They're going, well, do you have another address? And all of a sudden it's 20 minutes of your time and they don't even know what the problem is at that point, right? I'm just trying to log in, right? Vanguard, if that's who it was. So now you've wasted 20 minutes. They've wasted 20 minutes on a call. We heard yesterday from a major account. It's up to 50 cents a minute for call center support. So pretty soon you're in the 10, 20, $30 range for a password fix. And this is the ongoing infrastructure cost that these things have. So when we started this back in 2011, we started with three pretty well known industry luminaries, a guy named Michael Barrett who is the CISO at PayPal, a gentleman named Taher Elgamal who is very well known.

Albert Chow:

They've been on the show. SalesForcer.

Philip Dunkelberger:

SalesForcer bit before that, the Elgamal Cipher. So he was known in the encryption space. And then a gentleman named Ramesh Kesanupalli, who is the founder not only of the FIDO fast identity online movement of making it a standard, he was also the founder of Nok Nok Labs. In other words, we were funded to see if we could take this idea of building a plug and play capability to change the way people authenticate. And 10 years later, Apple, Microsoft, Google, there's been over 500 companies, members of the working groups that have helped build it, and now they're building it into the product. The W3C has put it into all the browsers so it is there and available at the endpoints for people to turn on and essentially replace passwords. And the latest thing, as I mentioned earlier, passkeys is getting a lot of press attention, because that's one of the steps in making this FIDO protocol work universally.

Albert Chow:

Okay, so when you say pass keys, I want to make sure, especially we've always, we've done surveys on our audience before and how many are you familiar with blockchain? How many are you familiar with security? And of course everyone knows a little piece of tech, but no one really knows it all. And so I'll say, let's assume that more than half of our listener base might know something about tech, but they might not know about passkeys. Tell me what's going to change in the future. You kind of hinted at in order right now for me to use my Vanguard app, I have to log into my phone, which has a password.

Then I have to log into Vanguard from my phone, which has a password, and then I need to do some form of 2FA right now, whether it's SMMS or I can use an authenticator, which by the way, I've used an authenticator before where I forgot to bring the codes over. It was like it took an act of God to get

myself back into my own accounts. I will share that for later, but that's how it is today. The way you make it sound is like I log into my phone and right then and there I'm fully authenticated in every direction. Therefore every service I use through my phone should just know who I am. Is that right?

Philip Dunkelberger:

Right? Not every service. Let's go back and take it forward about security. So let's take the design points of what this idea and what passkey does. FIDO the protocol, fast identity online protocol, it's now at W3C standard. It's built in the browsers. You can build an app on it, you can use the browser to interface to it. The backend system is what enrolls you. So if it is supporting the FIDO protocol, and FIDO works very much like a communication protocol. Let me describe it and then we'll jump into your ask. It works very much like a protocol. When somebody wants to enroll you in FIDO, basically the protocol says, hey, do you have a FIDO abled capability on your device on your phone? Is your phone FIDO enabled? Okay, was it built at manufacturing, which is the best way? Does it have a FIDO key on it or does your microphone have a FIDO key? Components in your phone can have it and have multiple?

Does your camera have a FIDO key? The point is FIDO at the endpoint, you can make any of those things FIDO enabled. And so your phone would answer back. You're just logging in like you usually do. Your phone would come back and say, yeah, I've got these seven items that are FIDO enabled and here's their characteristics, which is really cool. You can tell me the security level that they've been tested against. You then at the backend server, automatically, what computers are good at is go great, by our policies, we're going to enroll maybe two or three of those or only one. We're going to enroll your fingerprint reader or your camera. Okay? We're going to enroll that as the FIDO instance, and the next time you log in, it's going to ask you to take a selfie. And so what happens is when you log in next time, it will ask you to take a selfie.

Now there's a whole bunch of great tech underneath this for another time that's been proven. We've deployed this to literally tens of millions of people in places like Verizon and places like Mizuho Bank and like MUFG around the world where tens of millions of users are now using this to log in to their bank accounts, to e-commerce centers, et cetera. That's the idea of once I log in and I've been enrolled, I now have a private key that stays in my device, stored in hardware.

So it's the best thing we know how to do. And I have a public key. If you know and your audience knows public-private key pair, okay? It basically is using the best thing we know how to do on the internet, public-private key cryptography, to authenticate you. And I can come back and even tell the relying party's service environment, the finger, the phone, all of that in one pass because I bound you, your device, and the service that you were enrolled in. And to steal it, to mimic, to phish you, if I phish you and say, hey, click here and you click on it and think you're going to eBay, it'll come back and say there is no FIDO correspondent at this website.

Phishing. There's nothing to phish because you've got the public or the private key on your device in hardware and the public key is now in your account. There is no personal information that you send. Any of your biometrics or anything all stay locally in hardware, protected and encrypted. So we don't have these big password databases or these big databases of biometrics on the backend. It's one of the most misunderstood pieces of FIDO. Nothing in the biometric vein goes and gets stored on a database on the relying party. We reduce that, not only friction for you logging in, cool, right? You can log in now. And by the way, we can even take that a step further. Once we nest that key pair, because the key pairs don't transfer back and forth, all you're getting is a challenge.

The challenge says you should have a private key somewhere on your device in hardware and it should correspond to this challenge. You swipe it, done. If you nest that key in hardware, we can even take it without you doing that the next time you log in. So the point is we can literally remove the friction from

login and yet it's based on a much more secure underlying piece and you the user don't have to know anything about keys. You don't know have to know anything about databases. All that goes away. You just want to log in and get on with your life. Fundamentally, that's what FIDO is designed to do.

Albert Chow:

I got another question before we dive into how it gets implemented. Let's assume the private key's similar to, I have a crypto wallet. So if someone steals the hardware wallet, theoretically they have my key but they still don't have my account, my password and all this other stuff. Is that the same thing is if someone, so if I've authenticated my device on the FIDO network, if you were to steal my phone, that means you would still need to know my password. You would possibly need to know my face.

Philip Dunkelberger:

Here's the key to that. Let's jump in right there.

Albert Chow:

Yeah.

Philip Dunkelberger:

You don't need to know the password because passwords have gone away. The crypto wallet is, they've stolen your quote private key. The deal is the public key and then it's going to say, okay, the device is the person who logged in used a biometric, the person who used a biometric. By the way, we can set up a second key. Second key is we also have a seven digit pin. Okay? That's a secure pin that we've stored a public-private key on. We can take a third and say, hey, your device is no longer, you're now buying things and trying to do things with your device, move money with your device. We can send an out of band call to you and say, we're not getting the things. Now you can call.

Now you can call and try to get through the phone center and be qualified. The point is, there is no perfect security. Back when I ran PGP and most of your listeners will know what PGP is. PGP is probably the most widely distributed endpoint encryption software. The real key of that was if you could actually figure out a path, the pass phrase. Best case at scale, you could get maybe one attack, maybe one try. That's what the idea that we built in, because we came from PGP, so our security chops are reasonably good. The guys who built this and designed it were trying to make it universally hard for people to one phish do account takeover or do credential stuffing.

How do you credential stuff when you don't have the credential, right? I'm going to try to run a bunch of passwords at this guy's device, but I can't stuff it because he's using a public-private key pair to authenticate himself. It's a completely modern different way to go about doing it and it has a bunch of benefits that you can't do with traditional authentication. But to your point about you lose the phone? Without the corresponding servers and services and the way you logged in or what they asked for, the method face knowing all those things, you're not going to be able to do it, especially if it's a biometric. But the thing listeners have to hear is none of the pure biometric information is ever stored in the cloud or in a server.

Albert Chow:

Yeah, I mean the technical challenge, so the technical implementations is what I want to dive into next, but first I'll start with the user. This all boils down to what we talked about at the top of the show, which is we want it. We know that people, the proliferation of services is here. Everyone's going to be using

many, many services, many, many banking, many, many insurance, whatever. You're going to have tons of services, you're going to have passwords to everything. We already live in this world today. What Phillip's talking about is the future is going to be, when this becomes more widely adopted, is that login stuff that we do right now today, every single day, many times a day is going to go away.

You're going to log into your system one time. From there, you're authenticated, I don't know, every 24 hours, I don't even know how often I have to log in. But the idea is we can begin frictionless services, which we were joking about before we started recording. For example, for those of you out there listening, when you get hit with the CAPTCHA, because they want to know if you're a real person. It's about the most annoying. People are now saying like, hey, show me people that are doing something and you see all these different people. It's like Where's Waldo? I don't know how to solve these puzzles anymore. That's going to be a thing of the past, according to Philip.

Philip Dunkelberger:

That is what the industry wanted when we started this. So remember we didn't do this. Nok Nok Labs was the guys who took it and raised the money to see if we could even do this. Could we make it a standard? Could we put it on the standards track? Your audience is a group of people that range in the IT functions of people that want to know this. And people are saying, who's doing it? And you start saying, well, a lot of people are doing it. It's available today. This is not a pie in the sky. People in Japan where the use of biometrics was widely held both on phones and laptops for years. We have DoCoMo who we've got a full case study on of what DoCoMo's been doing because their problem was they had users they would advertise to, I have an advertisement of a new service for your phone.

And they'd make you go home, log into your laptop or desktop, order the service, put in a username, password, and a 14 character customer number. Kawasan, who is the CEO, said, why is it so hard to order services on a phone, right? Why? What can we do? He goes, I want a button that if I send an ad and you want the service, swipe your finger or take a selfie and then the service, we turn it on for you and we bill you for it. And that drives up the average revenue per user, which is the bedrock of M&Os, right? That's the bedrock of what mobile users do to get more money for the telcos. Fundamentally, that was one of the first big global instances of FIDO ever put out, the actual first implementation of FIDO we did with PayPal for payments, on a Samsung Galaxy five, that you could swipe your finger and essentially order you doing that.

That was the first global implementation of FIDO back in 2014. And like I said, today in China through our partnership with Lenovo, we have hundreds of millions of users around the rest of the world with known accounts like BBVA, Standard Bank, et cetera. These guys have all proven to their consumer base that FIDO can work at scale and it can work in a bunch of different applications. Now the really cool thing is that that's the beginning. That's what I call legacy FIDO. That's FIDO circa 2015. FIDO today for people like DoCoMo who've been doing it for years, they've got hundreds of partners that, hey, you've got FIDO on your phone? You want to come into a coffee shop and use your phone to buy? Swipe your finger. Because they're part of the ecosystem using FIDO now. And they've got literally hundreds of applications doing biometric based security or the user doesn't even know anything about that. They're just swiping their finger or taking a selfie and paying. No tap. No tap and go. None of that. Just great. I'm billing and going now.

Albert Chow:

So that's one of the things I have observed and some of my serving buddies have observed. Whenever we've gone into trips at Asia, of course Asia is known for adopting technology very quickly. What do you think is stopping or preventing or slowing down the process of maybe more North American companies

adopting this? Because you say it's widely, it's been available, like you mentioned, for more than seven years.

Philip Dunkelberger:

With us, it's been more than seven years. We wrote the protocol and introduced it, set up the alliance and fundamentally had a bunch of help in making it universal. The driver has been, if you ask me the drivers that have been stopping it, one is you make a great point. A lot of people just aren't educated on this. A lot of people aren't educated and they don't want to turn off things that work. We hate usernames and passwords. There's no argument on that. But they work, right? People know how to use them. User behavior's predictable and they work. If we want them to work better, oh, I know. Let's make you do SMSOTP. Let's make you do a bunch of other hoops to jump through as a user. And as you point out, that friction is stopping a lot of commerce.

That friction frustrates people. And that's why most of the people that are trying to use FIDO are really talking about new uses of it are trying to do employee stuff. When you're in behind a firewall, and this is my 41st year in doing this, I started my career with Xerox introducing this unique technology called ethernet in 1981. Ethernet 1981. Pretty well established today. Nobody even questions ethernet, but man, nobody trusted that. Nobody knew what it was going to do. And at the end of the day, coming all the way forward, this is like that. One, there's an education that it does work. It's being deployed all over the world. It's saving people money, password reset these things into it. We'll publish a study that we'll be happy to share with your users about how much money they're saving and things like password reset, how they're cutting login time, where they're doing right now, you log in and a lot of sites you notice you wait.

And if the web's busy, you really wait. We've cut their login time by about 70%. And that is actual dollars to their bottom line. The whole point is the IT guys here know that they can say to their users behind the firewall, you got to use these devices, this application we wrote and it's got to work this way. Okay, great. I work here. That's the rule. You can't do that to the global consumer. You just can't.

Albert Chow:

How fast are manufacturers picking up to this standard? Because you mentioned before, I need a device that of course supports it. Are the manufacturers jumping on board? Are they saying, hey, yo, we want to make devices with this? Or are they reluctant or what's going on there?

Philip Dunkelberger:

I think you're going to like the evolution of the story. We started with people like Intel, build it into the chip set.

Albert Chow:

Oh, okay.

Philip Dunkelberger:

Let's go to the best we can do.

Albert Chow:

Don't even talk to the phone makers.

Philip Dunkelberger:

Yeah, it's just a component that we need to be able to take a key from and create keys and drop them in. This key based idea is it was revolutionary because you get to all the edge cases very quickly. What about this? What about that? We've built it in things like Google glasses. We've built it in things like vests on a shop floor. So you don't want to take your gloves off, you don't want to get your phone out of your pocket? You can walk up and your vest authenticates you because it's got a chip set built in the vest. Pretty cool, huh? Opens the door. You want a manufacturing line? You want to hit the stop button?

Albert Chow:

Yeah. Yeah. Security protocol.

Philip Dunkelberger:

Security protocol of how do I stop the line? Well, you can do all of this with embedded FIDO. And I can take you through a bunch of that for another time. But the point is, this is really talking about the title of Passwordless Off. Passwordless Off is just the beginning of what this thing can do. And it's the protocol that allows endpoints to talk to it. There's over a 1,000 out there. It's supported by Apple, Google, Android, Microsoft. They're building products across the scale that support the protocol. So now you've got the ability to plug and play. Just the vision we had 10 plus years ago when we started this adventure. It's built into the infrastructure of the internet. And that's what people need. Remember when we had to put a dongle in to do WiFi?

Albert Chow:

I don't quite remember, but I remember when things change and you needed a dongle to do hard line. Yeah, I remember that.

Philip Dunkelberger:

But we used to have this thing before WiFi chips were built into laptops, you had to stick a dongle in the port. And this is like that. For years what we've been doing is saying, write an app, or us, because we'd started it, use it in the browser. We developed the browser capability. Because you can't dictate, 77% of transactions come through a browser interface, not an app. Remember the whole story about there was an app for this?

Albert Chow:

Yeah. And that's dead. That's not interesting anymore.

Philip Dunkelberger:

Yeah, we had to 10 years ago, support apps, browsers, et cetera. The way people communicate on the internet. But at that time they weren't using phones as the weapon. They were using laptops. And then all of a sudden people started using their phones for everything. Data, E-commerce, mapping, all the things you do with your phone. So we pivoted to the consumer space and said, we are the only guys building this. The vast number of users, and we had people like DoCoMo, a phone company, Verizon, a phone company, T-Mobile, a phone company, come to us and say, hey, can you enable either through the chip set or through the handset the ability for us to plug and play this FIDO protocol? And they were part of the alliance. And so we did. And that's the backstory of all of the 10 years we've been doing this, getting marshal in the industry.

It's been a long journey, but it's here today. And you can start not having to make your customers go through SMSOTP. You can put it out there for general login today. The more advanced things you can use it for in commerce and other areas, there's all kinds of regulatory things in the world, right? You've probably heard of PSD2 in Europe. Your users will go PSD2. It's this European banking authority says if you're a European citizen or outside the EU and you're going to do financial transactions, you have to support this thing called step up authentication. Oh good. What does that mean as a user? It means I've got to have the ability in the middle of a transaction for the relying party to say, hey, I'm not getting a good signal here from you. Step up. Give me a different method of authentication.

FIDO supports that, as I said in the beginning of the conversation, out of the box. So you start to see people, and back to your question of why it's lagged. People like Apple did not come to the floor in a big way until 2019. And what happened in 2020? COVID hit. And then everybody was worried about, we got to make our employees that are no longer in a building with a perimeter, we have to treat them like consumers. Well now, that's really change the face of computing. And people are saying, hey, everybody is just people out there, like I said in the beginning, with devices looking for services, whether they're an employee or whether they're a consumer, and I've got to find ways to manage both of them on the same platforms.

Albert Chow:

Amazingly. Oh, there's people looking for services. That is probably the best simplification of the 99% of us today. That's what we are.

Philip Dunkelberger:

I'm not the brightest guy in the world. Okay? I know what I do all day working out of my house.

Albert Chow:

Access service one, access service two, access service three, whether it's for work or whether it's for your personal life.

Philip Dunkelberger:

And it's not in a way anymore where you get to go, well, I think, remember the idea of carry two phones, carry two laptops? That doesn't work anymore either, right? Cost infrastructure, that just doesn't work. So there's just a bunch of these things that the protocol, and it's not magic, it's evolving. This passkey thing was an idea of, hey, if I lose my phone or upgrade my phone, Phil, let's say I've got 100 services that I've now created a key for, right? I've now created my private key for and I lose my phone. Well, what does IT always do? They have this thing called, oh, I'm going to hit myself in the head, backup and restore. What this does is it allows the manufacturer to back up and restore your key pairs. Cool, huh? That hey, if I get a new phone, they can load all my keys.

Now people go, well, does that do lock in? Am I locked into using a Mac or Microsoft or Android? Already, when the announcement of passkeys of backup and restore, that's just phase one. They've already agreed that they'll back up and restore other people's keys. And you kind of stand back and go, wow, do I want my keys to be done in this? I go, guys, you've been giving people your password sets on all these devices for years. This creates this massive attack surface for the backend. I mean, your listeners, Albert, I imagine are going, hey Phil, there's this new thing called attack surface. And I'm going, if you're in the anti-fraud business or any of those businesses, you've been talking about that for 30, 40

years. What is the attack surface we're vulnerable to? This reduces the attack surface dramatically for the relying parties.

Albert Chow:

And what I'm curious about is what's happening right now. And that's a big subject that we've had for the last few guests, because of course the economy's been on a bit of a boom, right, since 2008, the housing recession to now, and now it's changing. The direction is changing. There's a lot of economic uncertainty. We see a lot of tech companies doing layoffs. But at the same time, the battle for the consumer isn't changing. The battle for the consumer's still going to be an absolute, I'd hate to use the war analogies, but it feels like it. It's like business war, right? Everyone's trying to win the consumer, but at the same time, people are watching their spending a little bit right now.

Do you still see businesses opening their doors saying, hey Philip, come in here. Nok Nok Labs, come in here. Tell me how I can make my services better for customers. Are they still talking to you this way or are they saying, hey, this sounds like too small of a benefit, like too expensive. I don't want to do this right now. What's happening? Or for your marketplace, are people looking to do this still or are they starting to slow down like, hey, listen, I think that the user experience will be improved a little bit, but it's not worth it right now. I'm too uncertain about next year. What do you see going on right now?

Philip Dunkelberger:

That's a really great question. Actually, from this technology availability, has been a great question for a while. You ask why in North America versus regionally. Regionally we've seen uptake and continue to see uptake. We've seen rollout from one of our banks. We've seen rollout in who's the largest bank both in Southern Europe and Latin America. They rolled out to Mexico, Peru this year. They continue to roll it out because the cost savings. Cost savings first and foremost, but the interesting piece as we've rolled this out is what DoCoMo showed. They showed that you get better uptake. When friction is removed, users buy quickly and they buy more. When you remove hurdles to people that just want to get in, get out, get on with their life, like I said earlier, and we said, hey, just people looking for service and devices, this is what they want to do.

So no, we've actually seen the people that are deployed continue to deploy. We're having our best year ever and we're having more people. The US federal government came out with this executive order almost a year ago now. And nobody really paid attention to it. But the National Institute of Standards has been saying for years, we can't, as the federal government, as Global Fortune One for technology purchases, nobody buys more than the US federal government for tech in the world. And Global Fortune One is saying, not only do you need to go to MFA. When Russia attacked Ukraine, president Biden got up and had a multi-hour presentation and they brought the FIDO organization up to say, traditional MFA has got to go. Traditional ways the government's been protecting itself has got to go.

Albert Chow:

It can be intercepted, yeah.

Philip Dunkelberger:

It can be intercepted, it can be harvested, it can be hacked. And we see it every day. We've got to think differently. And the point is now Global Fortune One is saying, you got to use this. There's this construct called CMMC which are people who make commercial off the shelf products, cots. I want to sell trucks to the federal government. I'm Ford. I don't want to modify them. I don't want to have a government

mandated gas tank. I just want to take off the line and sell fleets of trucks to the government. They now have to have a standard because of supply chain and other issues that they fundamentally are secure in even selling cots to the government. There's over a million businesses in North America and overseas that have to meet that mandate just to sell to the federal government like they've been doing for the last 50 years.

Albert Chow:

It's funny you mentioned that, you're the first person I've heard mention CMMC since, because I know a gentleman by the name of Alli Bey and he is the CEO of a company called Totem Tech, and they have a whole business about CMMC certification. I was like, I can't believe. When he showed it to me, I could not believe, like you said, someone who supplies, let's say a non-smart non-digital product, safe product like blankets. If I supply blankets, I have to be CMMC certified? That sounds insane.

Philip Dunkelberger:

No, and you hit it on the head. What are all these people worried about? They're worried about fraud. They're worried about the things that all the data breach data shows. Look at what we're talking about. We're not talking about how badly governed FTX was. Right? Nobody's talking about that there was no governance oversight of the company.

Albert Chow:

They shouldn't. I want my money back. I lost $700, but I want my money back. I hear what you're saying. Weirdly, we're giving this guy SBF a platform to defend himself. I don't understand.

Philip Dunkelberger:

No. Well, whatever he's doing, good, bad, or indifferent to your point, trying to defend himself to explain himself, the real issue everybody's going, where's my money? Fundamentally, a lot of data breaches. Hey, I'm sorry your stock took a 20% hit because you had a data breach. Is my money safe? Did somebody steal my identity? That's all I care about. Just answer my questions. How do I fix it? How do I remediate it? And talking to an IT group of listeners, remediation is something that they live with every day. And we did a study with Larry Poniman Dr. Larry Poniman, who originated the cost of the data breach studies. And I asked Dr. Poniman, can you go ask these big vendors what failed authentication is costing them?

And he did a really unique study. His study was, I'm going to go ask the guys who support people on the phones, right? Guys who answer the phone when you got a problem with authentication, I'm going to ask their boss, ie the IT staff. And then I'm going to ask a lot of business people. So a lot of people, do you have a problem with authentic? No, we're great at it. You ask the guys that were managing the people that support, well, we're pretty good at it. You asked the guys on the front lines and they're going, it's horrible.

Albert Chow:

Oh yeah, we can't solve the problem. Who's solving the problems?

Philip Dunkelberger:

Who's solving the problem? And the only thing they agreed on at more than 70%, and this was 1,200 customers in Larry's database. Three people more than an hour of Q&A. They weren't doing a Survey

Monkey. This was real people he knows, people he trusts. The only thing they agreed on more than 70%, Albert, was we all agree that if we don't fix the problem really quick for people, we lose the customer. So authentication is never looked at as anything but a security play. And why people are figuring it out now, as people are doing these digital transformation projects in the UX and UI user interface and user journeys are not, the experience are not easy and there's more and more friction laid on them, you're losing customers. So we did this digital thing to improve our bottom line, to make the customers more loyal, better, et cetera. And we're actually losing customers at the point of authentication. That's nuts.

Albert Chow:

So one of the big things that always comes up in a software discussion between vendors and companies is this idea of the time to value. Well, how long does it take for me to get this value? And I don't quite understand because I've not lived through it and you have, but I have lived through this, which is if you install software, it takes longer to proliferate to its end users. And so if you install, implement a big change at a company and you have to train everyone how to use it, that takes a long time. You have to invest in training. It's expensive.

But when it's consumer level, you don't really have a way to train them. You just got to hope that they can pick it up and use it really quickly. And it takes time to proliferate. So you mentioned Intuit. Sounds like they're using it, banks are using it. So these are companies that might have hundreds of thousands, maybe millions of customers. They've deployed it. It's deployed in Asia to hundreds of millions of users. But if I'm a new customer and I've never done this before, how long does it take before I guess enough devices are using it so that I can get the value out of it?

Philip Dunkelberger:

That's a great ask, because right now the new companies, you said, are people still coming? We've got people going live from card networks to payroll networks, et cetera. And they're saying, hey, whenever you ask the user, and I think you know this well, when you get that question, hey, do you want to try this new thing when you're trying to log in?

Albert Chow:

The answer is no.

Philip Dunkelberger:

No, I just want to log in. Here's my username and password.

Albert Chow:

Yeah. They never say yes.

Philip Dunkelberger:

Yeah, they never say yes. And that's skip level capability. So I've got people that have said, when we register your phone, we're automatically going to equip that phone. When you register your phone, we're going to enroll you behind the scenes with the FIDO protocol. Just from day one, you use it, you're paying for it, we're going to enroll you. And anytime we want a service that's FIDO enabled, the keys are already in place. The infrastructure is taken care of it. That is what we've seen from an uptake standpoint of people using applications that are FIDO based. The easiest. It's just built in. It's there. We've seen two payment systems do things like, hey, I will give you $5 if you swipe your finger right now

or take a selfie. And what you're going to do from now on is log in and do that and we're going to give you five bucks just for doing that to be enrolled.

So there's incentive based. Okay? One is on the one end, we're just going to do it and enroll you and have that infrastructure play. Okay? The other end is we've got people paying people to be enrolled because they already know the financial benefit of these people not calling their help desk. We've reduced a couple of different companies help desk calls on this to near zero because password reset is, hi, I'm going to swipe my finger or I'm going to take a selfie again and create a new key. That's the beauty of this is that this is all stuff that is no longer backend based. This is designed truly to plug and play. If you've already got risk scoring engines on the backend, in our product, you can basically employ those and say, hey, we want to know our total picture of who's there. What is the risk of this transaction?

Good. Make that part of before you authenticate. Make those checks that you've already paid money for usable in this. But the real capability is I'm not sending you a key to carry around on a dongle to plug in to log into something. But if you look at the regulated industries and you look at the capability that they need to get you the services you want, and they might have multiple. Do you have multiple services with your bank? You have a checking account.

Albert Chow:

Of course.

Philip Dunkelberger:

Car loan. Yeah, everybody does. How much of a hassle is it when you go to log into that where they haven't federated your login? Well, log in when it's on off one time passwords. You can't federate those. With FIDO, it's key based. I know the key. I know the user. I know it's Albert because I enrolled him.

Albert Chow:

I didn't even know that you said it can't be done. Because I'm thinking that I was literally just thinking as you were talking about how on my MX account, I can log into my MX credit cards or I can log into my MX savings account. But I can't seem to log into both. I guess they were two services from the very beginning and they're not merged in any way. I have to log in twice. Super weird.

Philip Dunkelberger:

Well, think about if you use any of the services like TriNet. I use TriNet as a-

Albert Chow:

I used TriNet too. TriNet, yeah. They just moved 401k providers.

Philip Dunkelberger:

How much fun was that?

Albert Chow:

They didn't recognize me last night.

Philip Dunkelberger:

Did you change from last night to today? The answer is no. I'm out here. I'm the same person. But all of a sudden they don't recognize me anymore. And this is the real conundrum of having to figure out how to do differently. Like I said, DoCoMo has shown over the last five years, published a case study on it. We can do hundreds of different logins with thousands of different devices. Based on the strongest protocol, public private key challenges we know how to do. It's privacy preserving meaning there's nothing that anybody can hack off your device. Public keys without private keys and inverse don't work without each other. And the device and the service, as I said earlier, it's called a three-way bind. We are the people that said you should use this. And fundamentally it's being done now. And to your point, you and I could sit here and riff for hours about trying during especially the Christmas period of how come I can't just log in and buy things and move on?

Albert Chow:

Yeah. I mean, I'd argue that that's the number one reason why Amazon has gotten such big market shares. Because they've just made it so easy that people have just adopted it. Because one of my friends, and I've instantly noticed as well, because I'm a cheapskate, is that they don't even have the best prices anymore. But they've made it so easy that people have forgotten that other places exist to buy products and services. They're just like, I'll just go over there. They go with by default.

Philip Dunkelberger:

Study just came out with people saying from payments. If you know the payments folks, Karen Webster, her husband have got a great website. But she just did a study, a couple thousand different businesses saying the number one thing they're hearing is after the pandemic was it's all about ease of use. It's all about accessing services quickly. And I'm not going to move it because I know how to use it back to user behavior. We're not altering end user behavior. And the thing Amazon did better than anybody is, like you said, they don't even have the best prices anymore. But we use it because we know how. We know we've got a good selection. Let's get in, get out, get on with our life.

Albert Chow:

Exactly. Exactly. And despite the fact that I guess fraudulent products are occurring more and more often there, people still have such a high trust factor with that company and they just continue to purchase there. Well Philip, man, we're running low on time, but this has been an amazing conversation. I love hearing your perspective on simplicity and you did a great job, in my opinion, of explaining a complex subject. Although if you test me, I might get an F. I think I understand.

Philip Dunkelberger:

After 10 years, I'm still learning every day from the customer setting and other people.

Albert Chow:

I got my first crypto wallet recently and I was like, what do you mean? The key is the thing? And I'm like, but it's got a recovery password so if I lose the key, I can actually recover it. But if I lose the recovery password, so I'm like, ah, is it safe or not safe? I can't figure this out.

Philip Dunkelberger:

Well, back to your point, this whole subject matter, we actually looked... Nok Nok was always the dark horse for naming the company. The leader for three rounds of the naming environment you do in marketing was vast. This thing is so big, we should just call it vast. Everything authenticates.

Albert Chow:

Yeah. I think your name works better as Nok Nok Labs. Because once you hear it, it's just memorable. Reminds me of, for those who haven't read Shoe Dog, Nike story, Phil Knight, he wanted to call the company Dimension Six. Someone's like, doesn't fit on the shoe. Let's change it. Yeah.

Philip Dunkelberger:

Okay, we'll default to Blue Ribbon Sports, right?

Albert Chow:

That's Blue Ribbon Sports. Yeah, that was his next idea. Well, we're Blue Ribbon Sports. We should do that. Someone's like, well, let's call it Nike. It's like, yeah.

Philip Dunkelberger:

I'm not the marketing guy, I just make shoes.

Albert Chow:

There you go. Well Philip, man, it was great having you on the show. But before you go, we want to do the lightning round. The lightning round is brought to us by Salesforce platform, the number one cloud platform for digital transformation of our experience. Philip, this is where we ask you questions outside of the realm of work so our audience can get to know you a little better. You ready?

Philip Dunkelberger:

Happy to do it.

Albert Chow:

All right, let's start here. What is the most unusual, and it can't be password related, all right? What's an unusual IT problem you solved in your life?

Philip Dunkelberger:

I think I would probably have to go the most unusual problem that we've found was back in the PGP days of what people would encrypt. And then to your point, forget their passphrase. And we finally came up with PGP Universal, a way to store and manage keys. And one of the drivers was how many people are calling support and going, I lost my passphrase key. Well, is it really important or do you want to create a new one? Or what do you want to do? Right? Support call. No, we have our entire family history and everything and a bunch of our financial information on a disc and we encrypted it all and now we forgot it. And kind of like, in 100 places in the product, 100 places elsewhere. Don't lose this pass phrase. So backing up keys, backing up and restore again.

It's really an important process. So yeah, the stories you'd hear, some of the cases, the most unusual case is a sad case where they had a guy that had actually committed a murder and he had encrypted all of the files. And the scary piece was he had been murdering children and they were worried that on his

encrypted hard drive, by the way, the guy had a master's of science and computer, it's a true story. And the FBI was going, can you break this? And the answer was no. There was no backdoor skeleton key universal key for PGP. People who know that know that well. But what happened was they cut a deal with the guy to finally give up his pass phrase. But that's one of those true tragic things that was going on because he had pictures and lists of kids, like kids coming and going from school. And they didn't know if those kids had been in danger. Just a really deep, black, dark subject of the dark side of both technology and the internet.

Albert Chow:

What brought you, I guess, into security? Because that's a dark story, and then of course most of those conversations have been positive and hopeful. What brought you into technology and what got you into security?

Philip Dunkelberger:

I walked in the door at Xerox when I was out of college and they were trying to hire new people because of new ideas. They were trying to train copier and duplicator salespeople to sell technology. When those guys were used to walking in, if you think about Xerox 1965, hey, what's this thing do? That's a copier, right? Nobody'd ever seen one.

Albert Chow:

Why would I use this?

Philip Dunkelberger:

Yeah. 15 years later they're the fastest company in the history to do a billion dollars in sales or something. But now they're trying to sell networking where they introduced the Palo Alto Research Center. And they found that if they could hire people out of college and train them essentially in computer science, they would be better at understanding customer problems. So how I got into it was from the beginning of trying to understand customer need and then applying technology to solve the problem. I got a call years later, Phil Zimmerman, who is extremely well known to anybody in the internet age. He's on the second cover of Wired Magazine. Phil was doing this thing called PGP where he was trying to take encryption to the masses so we could whisper on the internet. And even though I'd been at Symantec when we got into security, some people don't remember that Symantec did not start as a security vendor.

Albert Chow:

What did it start at?

Philip Dunkelberger:

The name. Semantics.

Albert Chow:

Okay.

Philip Dunkelberger:

It had a natural language database called Q&A which has gone long gone, but it was one of the most popular buy it Q&A. And for the guys listening, gals listening that remember that, Symantec evolved into a utilities company and then they evolved again into a security company. And I was the VP of sales that was responsible for that particular area. But in my background from Xerox, I went line staff. I was the X&S product manager, Xerox network services product manager. So I was a network product manager in my career. But all of this was about solving customer problems. How do I keep data secret on the internet? How do I let you keep your file secret? And ultimately, this thing was the greatest challenge that I've ever tried to take on was there's a hole in the internet called username and passwords. There's a hole in the internet about identity. Can we build a bridge between identity and the way you go about establishing that to fix that problem?

Albert Chow:

Yeah. Well, we look forward to you figuring it out because I think I speak for everybody, we're passworded out. We got too many, we got too many. And as you know, many people have just defaulted to, well, I'll just use the same one for all of them.

Philip Dunkelberger:

Which leads to the number one thing that leads to account takeover. Some guy hacks a database and just run it at a couple hundred thousand people and I'm in the money. Really cheap way to be in business.

Albert Chow:

Yeah.

Philip Dunkelberger:

So what else you got for me? That's why I want to solve problems. That's what we've done.

Albert Chow:

Well, Philip, it was awesome having you on the show. We're out of time. But you are absolutely right. You are full of knowledge and I love the way you explain what I think is a complicated subject. Maybe to you, it sounds like it's the back of your hand, but even you were able to admit that, hey, you're still learning stuff as we go. And listen, we look forward to you figuring this problem out because like I said, I cannot wait to the day I don't need a password.

Philip Dunkelberger:

That makes you, me and a whole bunch of other people, I'm sure. So thank you to your listeners. I hope it was worth the investment of the hour of listening to our conversation.

Albert Chow:

Awesome. Thank you for joining us today on IT Visionaries.