FEDERAL TECH PODCAST

Fraud, Identity Theft, Federal Systems

Welcome to federal tech podcast. My name is John Gilroy and I will be your moderator. Our guest today is Wes Turbeville. Vice President federal at ID me. And today we're going to ask the challenging question that was first brought up in a 1978 album called Who are you? So as that might have been born, might have been before you were born? How do you remember that album?

01:28
I do not. That was before I was born. Wow. Super excited to be here. Yeah,

01:33
yeah, there's a there's a group back then called the who and they had an album called Who are you? Maybe it was prescient, but but that's what's going on today was asking Who are you? I think this question has gotten more and more popular ever since the pandemic. So Wes, give us all about your background, and you have kind of intriguing background and some dangerous things in your past. And then tell us about a little bit IDB we'll start this conversation off.

01:55
Yeah, absolutely. John. So Westerville, like you mentioned, Vice President of federal aid, it may prior to joining it me was a consultant at McKinsey and Company for about seven years focusing on public sector operations. And I did that both in Europe and in the US. And prior to joining McKinsey was a test pilot in the Navy. So had been around the federal space, federal technology, Federal Acquisitions, and helping the government just do things better, pretty much my whole adult career.

02:20
Good, good, good. Yeah. Everyone loves to talk to test pilot, because we know they're on the edge there, huh.

02:25
I often explain to people a little more right stuff and a little bit less Top Gun. The way I like to explain it.

02:31
I have a grandson who's little bit over two and two years ago, they came in to live with us during COVID. And lot of things changed two years ago. And I think in the world of identity identity management. This was a what would Malcolm Gladwell call it a tipping point, a changing point because all of a sudden, no one was taking the metro into work. They were trying to communicate and had to change all kinds of things identify themselves, where they were in the federal government, where their federal contractor or just a commercial device so so when you look at you know, the last five or six years, you see this, would you say this is one tipping point. And we had to take respond to some of this and improve the ways we identify people online? Is that right?

03:06

Yeah, I absolutely think that's right. And, you know, I think everybody knew the transition to digital services was going to be coming. And I think the pandemic greatly accelerated that McKinsey has done some studies and some work, to put down a number that estimates essentially how much the pandemic accelerated the transition to digital services online. I think their number is on the order of four to five years. And what they saw that it were, the acceleration happened was different across different segments of the economy. And one of them where it was the greatest was actually in the public sector. And so I think that's what's driving a lot of the debate and a lot of the attention right now on, you know, the push to make the government modernize faster than it's traditionally used to moving and bring citizens online so that they can gauge their government that way.

03:51

You know, it's awful hard to paint this in broad strokes, although I love to interviewed the Chief Technology Officer at US Patent trade office, and, and he said, hey, no problems with us, because most people remote before pandemic hit, they made a very easy transition that no pun saw. But this isn't true for everyone. And people have had to start thinking and changing and and, you know, I've done a lot of interviews with software developers and talked about cybersecurity, and in my world is CSP as a cloud service provider, but in your world, CSP is is a credential service provider, maybe just tell our audience what the heck that means.

04:26

Yeah, absolutely. So it me is what we call a credential service provider. We issue portable, trusted digital identity credentials for our users. And we do this in accordance with the NIST standards. And our adherence to those standards is audited by and reviewed by an outside independent accreditation body called the Cantera initiative. And so once you sign up with ID me and you have your il two credential, you can then go use that credential anywhere that accepts an IL two and so if you verify your identity with me One government agency, you can then go login and another government agency with a simple, frictionless already established multi factor authentication pathway. And so you know, and use that anywhere it's accepted. And what this does is it, you know, improves the customer experience for the end user, because you only have to verify once, and then you can access anybody that trusts that I sell to. And it improves the level of trust for the government agencies, because they know when you show up with that I sell to that you are who you say you are. And then it also reduces costs. Because now to visit multiple agencies, you don't have to go through a verification process at each agency. And so it actually ends up being a cost efficient way to approach the problem for for agencies. And one of the just sorry, one other thing to mention, one of the great things about it me is because of our work across the private sector, state and local and federal, that credential is honored across all three of those sectors. So even if you verify it, IRS, but you have work that needs to get done with wherever you live, say the state of Arizona and they accept an IL two, then you're going to use the same credentials with both your state and also your federal agencies that you interact with.

06:14

You know, Wes, you use the term trippingly on the tongue, you know, I will too. So is this contrasted with like a legacy approaches or so what is this contrasted with? Or when did this whole change take place?

06:25
Yes, sure. So il two stands for and I'm sorry, I know, the government is very familiar with acronyms. But you know, there's always new ones to learn. But il two stands for identity assurance level two. And its definition is laid out in some NIST digital identity guide guidelines called Special Publication 863. Three. And what happened is back in 2017, in light of a lot of data breaches, you know, there was 147 million Americans in Equifax that had their data breached 22 million for OPM. 50 million in recent breaches with with T Mobile. NIST essentially said, Hey, knowledge based verification is probably not safe anymore. Because your information is out there, the old way of doing things like asking what kind of car you drove in high school, or what address your your parents live at just isn't going to work anymore, because that information is out there. And so they revised their guidelines, they released the dash three, and one of the major changes in the dash three is it moved off of the old level of assurance, and moved on to a new identity assurance level for for proofing activities. And one of the big steps in that is that to reach il two, doing it remotely. So over a digital channel, you have to collect a certain amount of evidence in order to issue that credential. And then you also essentially have to make either a physical or a biometric comparison to the strongest piece of evidence. And so what this does is this means it's not enough to just have your information. You've got to have somebody's information, copies of their documents, and then also a copy of their biometrics in order to, you know, spoof them and have their credential issued in a fraudulent way. And what most folks use for the biometric portion is is a selfie. And I'm just because camera phones are pretty ubiquitous, and you know, available, you know, most people have access to them. NIST also mentions fingerprints and iris scans in the guidelines. But I think the the biometric stuff that most folks are comfortable with is the is just taking a selfie.

08:34
Good. So we use the term URL, you think multifactor authentication MFA. So this is just part and parcel. But multifactor attending was was probably part of the older way of identifying legacy application, wasn't it?

08:48
Yeah. So you know, the original way to secure an account was with a username and password. And when it became very clear that passwords alone aren't a safe way to secure an account. We started introducing multi factor authentication. And the way I think about it is, you know, this requires two things to access an account. And it's typically something you have. And something you know, and the way that most people engage with multi factor authentication today, is by receiving a one time passcode via text to their smartphone. So there's something you know is your password. And then something you have is your phone. And when you receive a code to your phone, then you can use that, that code to log in. But even that is under attack, and is no longer the safest way to do the second factor of authentication. And so what you see in a lot of zero trust strategy that's, that's coming is a push for phishing resistant and better ways to to, you know, essentially get that second factor of authentication. And that's why it may, you know, we offer six different ones, including push notifications via an app and secure keys and phyto two tokens as other options.

09:57

A lot of people don't like push notifications are but I'm not going to didn't always a lot of details on that. But I'll talk more about this multi factor authentication and, and people are, you know, I saw press release was the other day I look it up here on the air. There's some major companies that finally admitted they're going to try to get away from passwords. So does this fit into discussion here? Is that a whole separate topic completely?

10:15
No, it does. And I think NIST actually has guidelines on this. So in that same special publication 863. There's a sub chapter of it on authentication, and they talk about authentication, assurance level three, a two factor authentication would generally fit under a L two, I think what the Apple and Google and Microsoft so the world are staring at with this passwordless authentication is getting to an ale three, we're obviously monitoring it closely, to figure out how it's, you know, it'll, it'll work with our platform, and then also looking at how this might react, and how they might reflect either this or other guidance in the next iteration of their digital identity guidelines.

11:03
So let's get away from the big fancy acronyms, and impressing people with all these words like zero trust and everything else. So I'm walking down the street, and got my phone out, and I get a message and it's my bank. And let's say it's the Wells Fargo. And Wells Fargo says you're in big trouble, you got to get that you're being attacked. And so just give me a real practical deadline. Like we're walking down the street in Atlanta. This is how it happens, John, we'll go to baseball, you know, the Braves baseball game or something. So this is it's it's not as sophisticated and accurate. It's just really simple, basic social engineering business, like, Oh, my bank called, well, if it's my bank, of course, you're gonna contact me. So I have to respond. This is how people get lulled into something.

11:44
That's right. And then the fraudsters notice, and they know this is a world full of distractions. And they know that hitting you at random times is when you might have your guard down against scams, right. And so the scams are getting sophisticated. I know some of the law enforcement agencies have started adopting the term whaling, which is a particularly advanced kind of phishing, where they're sending very personalized messages, by leveraging information that they already have about you in order to tailor the message and encourage you to respond. And, you know, the bank account, one is one that we're seeing more frequently, during the pandemic, the scams that we saw the most were related to jobs. And that was pretty obvious, because there's obviously lots of Americans out of work and very vulnerable. But then also a lot of romance scams, which was taking advantage of the fact that people felt pretty isolated during the pandemic. And so, you know, jobs and romance scams are the ones we saw the most starting to see more from the financial aspect as well. But it's, it's, it's pretty common, or more common than a lot of people might realize, you know, the height of the pandemic in 2021. And a summer, what we were seeing was around 45,000, folks a week coming through having been socially engineered, and it's something that we put measures in place to protect people, and to stop those acts when they're happening.

13:10

No, I, when I've done research on phishing, you mentioned earlier, I think it's a number I'd say, like 95% of the attacks take place through emails that correct or or I'm just assuming it's going to be text based, but it's, it's email based as well, isn't it?

13:24

It's birth. I think the fraudsters are realizing they've got to get to you through multiple channels. You know, I know, I'm personally seeing more via text than via email. And a lot of us because emails are getting more crowded. Yeah, you know, I, when I think about my Gmail, I have all the filters on, but still, it gets pretty crowded in there. And I'm probably more likely to respond to a text. And I think I'm probably not the only one that feels that way. I think that there's probably a lot of folks out there that you know, live there live their lives that way. And, you know, have those is preferred channel.

14:00

I teach down the down the road at Georgetown. And about a month ago, I gave a lecture about speed of websites. And what Google says is that if you're on a handheld device, and you try to read a site, and if it takes more than three seconds to load, 53% of the people are going to bounce. And so you have this dilemma between speed and ease of use. And and so I think this can happen in many identification challenges is that they need access, but they want to have it's fast. And so what I mean, so the solution that you're talking about here, is this increased speed with accessing a site this decreases in service because the speed issues

14:39

and by process, you mean the actual verification process? Yeah, this is so I think the answer is yes. In this on demand right now, economy and world that we live in. You do have to have a good experience in whatever you're doing. And so this is why we think that the portable model of identity verify wants in then have frictionless access wherever you go, is the right way to do it. Because, you know, in the old world, if I wanted to conduct business with three different agencies, I might have to verify my identity in three different ways. But in the new world with a portable identity, you can verify it once. And then there will be some friction, that comes with some security that you need to have some level of friction to make sure you're only letting the good guys in and keeping the bad guys out. But then once you've got that credential, as long as it's portable, it's standardized, and other agencies recognize it, you can then go use that credential in lots of different places using just that simple multi factor authentication pathway that we talked about. And so, you know, the fastest way to capture an audience and make sure that they engage is to take the friction out.

15:47

That's the word I was seeking friction. So you can call friction, waiting online for a telephone or delayed getting a website or having an identifier and so that it reduces friction so that that's a good approach. I think it was a good one. So let's say I'm starting with conferences, and going to conference on May 25, and the Washington Convention Center, and I meet people all the time, if I meet a federal CIO and start talking with them. So what kind of questions should they be asking people in the identity community about improving their security? And not, you know, delay, having no delays and button increasing? At the same time? What kind of questions should they ask?

16:24
Yeah, I think there's three big questions or groups of questions that I would encourage CIOs to asked. You know, the first one is really understanding the model of their identity provider. I think the second one is around how they help users with small digital footprints. And then the third one is around privacy, and users controlling their data. And I'll double click into each of those for a moment. On the first one for how their model works, the way we think of it is there's really two models of identity verification out there. There's what we call a consumer centric model, like it me where a user prevent presents a certain level of evidence that we then use to make sure clears the bar for the next aisle to and then we issue that credential. There's another model out there, that involves doing data brokerage, and collecting data, and building profiles on individuals that are then used to essentially verify their identity by checking information is provided against records in the background. And this much more passive, profile based model of digital identity, you know, introduces some additional concerns that I think CIOs should just make sure they're aware of, you know, number one being where those solutions get their data from, you know, number two being, what level of transparency and consent, they're using the the consumers and users have, but that data is being collected. And then third is how a user can opt out if they want to, because many of these profile based models essentially only allow you to opt out, if you're, say, an elected official, or you can prove that you have risk of physical harm. And so this is one of those things where I think it's important for CIOs, just to understand that there's a couple of models out there, and make sure they understand the trade offs of what those different models are. And as I mentioned, you know, it may was essentially born out of n stick the National Strategy for Trusted Identities in Cyberspace, and NIST grant funding, to launch a consumer centric model of identity verification. And in order to get that grant funding, we had to show that we were privacy enhancing, secure and resilient, interoperable and also cost effective.

18:56
I did some research for this interview this morning. And the couple agencies I think, have very sensitive information, IRS Social Security, they're involved with something called an identity federation. So So what is I don't what is that anyway?

19:12
So identity federation, is the idea that how do we actually make the credentials as portable as possible? So that ah, one agency's credentials, you know, develops a certain credential? How do I make it so that it can be recognized elsewhere? And one of the cornerstones of Federation is the government standards, you know, as they're currently defined by NIST, and essentially adherence to those standards. And as it exists today, you know, the, not all federal agencies follow them in exactly the same way. And so I think there are some, some things that we can do is, you know, as a government to increase Federation, increase the portability of credentials, and then ultimately, save money and also improve the user experience for for the consumers of America.

20:01

We can look at the past and see what happened during COVID and the pandemic. And it's always hard look in the future. I'm out. I don't know how you can, but if you want to look in the next four or five years, so I think some happened to prevent identity fraud down the road.

20:16

Yeah, absolutely. So think the threat is going to evolve. And I think what that means is, we're going to have to stay one step ahead of it. And what I mean by that is, many of the fraudsters that essentially made a bunch of money during the pandemic, have reinvested in their business. As you know, pandemic benefits have slowed down, they're now looking elsewhere. And I think you see evidence of this with some of the articles that you see coming out of the financial sector. So PayPal, four and a half million, fraudulent accounts. Zell having all kinds of issues with scams, you know, even heard Elon Musk, talk about authenticating all humans on Twitter as one of the things that he wants to do. Once he's, you know, once he's an owner. And so I think the only way to stay ahead of these threats is really close public private partnership, I think, you know, there's a lot of innovation that can be driven in the private sector. And that comes with, you know, competition, and also the right regulatory environment. So allowing the private sector to innovate, having a good competitive market, and then having the right guardrails in place, to make sure that the right models are being developed is really the best way to stay ahead of the fraud. And I think, you know, encouraging things that are going to help the consumers. So, you know, adoption of social engineering controls, and, you know, maybe there's a world where there could be additional guidance on that. And credential service providers are, you know, asked to provide additional controls from a social engineering standpoint. Doing more education in the market, and the American consumers, maybe there could be reporting of scams and more organizations like that in a theft resource center that get out there and help consumers raise awareness of where the scams are coming from, and what they can do to avoid them.

22:22

Now, there are people who are trainers in the cybersecurity area, they say, you know, you can take 100 people in a room and give good presentation, and 96 are gonna go away and learn the lesson, there's always going to be for people that are just, I mean, it could be afford, it could be for people in Wisconsin, for people in Brazil, for me that apparently uses for people rule that you can tell them the stove is hot, and they're still going to touch it burn their hand. And so is it gonna be automation the future? Or, you know, I guess I've seen a lot of humans do dumb things in my life. Do you think this for is maybe that's too high?

22:59

How do we how do we protect people from themselves? Right? Yeah, I think it's a great, it's a great point. And what I would say is in order to, you want to give consumers choice in whom they trust, but then you want to make sure that that choice is among things that clear a bar or meet government standards. And so I think removing some of the choices that you mentioned, like making multifactor authentication, the default. And the standard is really important. Making social engineering controls for credential service providers mandatory. I think, making sure that federal agencies adopts the standards that have been written by you know, the, the smart engineers at NIST is a good thing. And so I think giving consumers choice in whom they trust will make sure that the market innovates but then putting the right guardrails in place is the best approach.

23:55
I made this silly example already about a Braves baseball game, I pick up my phone and Wells Fargo. So is Wells Fargo or truist. Are these big banks out there? Are they credential service providers? Are they use credential service providers?

24:09
No, they typically use them and they have they have a role. You know, one of the things that you can do to help verify an identity is just using micro deposits in an account and so they have they have a role to play but they're typically not credential service providers themselves.

24:26
When it comes to the federal government are are there conferences that are coming up or the way that my webinars perhaps and be videos? We have a lot of people want to learn more and maybe the listeners podcast two months down the road and I want to learn more are there what do you think Cisco were suggested? Learn more.

24:45
Yeah, I think the great starting point is the Atomy website. If you click on our insights tab, we have a lot of elements

24:53
is ID dot m e so at Mass talker their fellow id.me Ha

25:00
ID dot May. And we have a lot of great insights on our pages, we have some that essentially, give those consumer tips how to stop the scam. We have some explainers on you know what I L actually means and the role that NIST plays in that we have some discussions on what it takes to increase access and equity and security at the same time. That's something that we've been able to accomplish in one federal agency and the Washington Post even wrote about it doubling pass rates, including minorities and less affluent, and we also increase security at the same time. And so there's some, some white papers on, you know, what it takes to actually do that. And so that that would be the first starting point for me. I think, another good website, and I mentioned the identity theft Resource Center. You know, from a consumer standpoint, that's a great place to steer people. You know, they they have a lot of data on what's breached, what kind of information is out there as floating around, and then what steps consumers can take to protect themselves?

26:06
So are you are you optimistic? We talked before the interview started? Do you have children? I have three grown kids. So when your kids are your age, do you think this is going to be a problem, the rearview mirror? Or do you think it's still going to be around for decades?

26:22

I think it'll always be around, there will always be people trying to steal from other people. But I think we are going to be in a much more secure world. And I have no doubt that it me is going to have a big role in that. And the reason why I have confidence in that is, you know, number one, we still continue to innovate. And our products are evolving to stay ahead of the threats, like I mentioned, you know, when social engineering was popping up, we put controls in place. And that 45,000 a week that we saw, is essentially zero today. We also have figured out what it takes to bring people online that don't have a large digital footprint. And so, in the past, you know, we know that the Consumer Financial Protection Bureau has said that around 45 million Americans either don't have or have insufficient information in their credit reports. And that means they're not able to get online digitally, where there can be more security. And so we've been able to do that through our omni channel approach, where we offer people who, who shoulder verify themselves through digital channels to enter a video chat, just like we've all done in the pandemic economy and verify their identity with some documents that way with one of our video agents. And that's had tremendous success. It was first launched with Veteran Affairs back in 2019, to help veterans living overseas and veterans with thin credit reports. And since then, around 4.4 million people have verify their identity through this video chat pathway. And these are people that would not have been able to get online otherwise.

28:01

That's the word used earlier equity. Yep. Yeah. And I think when I think of legacy, than I think of equity, it seems a has to be a transition or a newer way of doing things in order to make the playing field level. And, and when we look at the veterans, and I know the founder of your company, is a veteran, and this would motivate him initially it was he got very frustrated with I think processing a claim or something. And, and, and all of a sudden, in the early stages of your company's history, the veterans were, they're having a hard time and he came in and he helped them a whole lot. And, and I never thought of that were 10 years ago as an equity issue. But it really is, is of all the people, someone who's the veterans got injured serving their country, they should not be at the bottom militia should be at the top of it, should they?

28:45

That's right. And that mindset of helping people get what matters to them and helping people get what they deserve, really runs through the culture of it, me, I'm a veteran myself, I use my credentials to access the VA. And then, you know, also access other government services. And so my wife's also a veteran, she uses her ID new credential access VA, and so it's something that runs through her veins here and you know, is is really ingrained in the culture and something we're really proud of.

29:13

Yeah, I visited veterans hospitals in Oklahoma many times. So I think I have a little bit of empathy for some of those situation, blame me bad situations. I mean, just because you and I are familiar with technology doesn't mean someone in rural Idaho, is that familiar? And they may not get what's owed to them for their benefits. And it's just it's it's it's really got it's got a technical aspect to it, but I think the story has got a human aspect to it. And I think that's, that's what you guys have managed to do it. Id me I was reading some blogs this morning. If you can humanize the story and say, Look, this fella, this poor West here served his country. He's in rural

Nebraska, and he didn't realize he qualified X, Y and Z because of some, you know, hiccup with identification with the IRS, and you know, it happens

29:59

yes. And, and everybody has a little different scenario or situation. And so this is why we actually think it's really important to have really good algorithms. But knowing that they can't touch everybody, you've got to back them up with people. And so we bring Best In Breed algorithms together with human reviewers to get everybody we can through the pipeline through the funnel. And the way we do that is when folks fail or check on ourselves or flow, we have real time human checkers that can come in and take a look and keep people moving through the process, if we can't get him through that way. And we have them join a video chat with a human just just like everybody else has had a meeting in a pandemic economy. And then if that doesn't work, then we can also go to an in person verification option. And that's one that is available in 650 retail locations around the country. And the way I think about it is this is the ultimate relief valve for people that you know, either struggle with the digital channel, or people that just aren't comfortable with it. And, you know, it's something that we think it's important to have all three channels, digital, video, and in person in order to meet people where they are, and be able to bring as many people as possible online.

31:17

Yeah, know your audience. That's what the marketing people say. This has been a very enlightening discussion, I learned a new acronym CSP today get to flash that around. You've been listening, John, you've been listening to federal pet. You've been listening to the federal tech podcast with John Gilroy. Like thank my guest, Wes Turbeville. Vice President federal ID me that's the story.