FEDERAL TECH PODCAST

# Identity Management and the Federal Government

Welcome to the federal tech podcast. My name is John Gilroy and I'll be your moderator. Our guest today is Matt Thompson, General Manager of Public Sector solutions at Souq here, Matt, how



01:48
are you? I'm doing great, John, and thanks so much for the invitation to join you here today to talk with your audience about this really important topic of identity management and how we enable better access for the public to government services.

02:02
Well, I tried to do my homework, you know, I'm in the classroom, help my students do homework, you know, sign up this morning. I like a little piece of paper and a pen. And I started looking at all Matt Thompson, and I ran out of ink. Oh, my goodness. I don't know how old you are, Matt. But you've done a whole lot. And if you use it been around I see this VM I see this service overseas, I see his Harvard MBA I see this that I don't know I see patents. So just just give us maybe a quick, brief background and how you wound up working for so cure.

02:32
Sure. Thanks so much, John. And, you know, I not big on talking about myself. But you know, my background is kind of relevant to how I got into the identity space, which I knew nothing about when I was separating from the military. Gosh, 14 years ago, now, I served 11 years in the Army. Most of that time as an Army Ranger, I did four tours over in Iraq and Afghanistan. A lot of that time under General McChrystal, who many of your audience would probably recognize, as part of Joint Special Operations. But um, you know, when I was leaving the military, my business partner at the time, and I saw how challenging it was for members of the military to prove their identity online, a lot of the military discounts military benefits were restricted to in person locations, and requiring veterans to show up with a lot of paperwork in order to prove their eligibility. And we just thought that, you know, there was too much personally identifiable information being exposed by veterans to claim something like a 10% discount at Under Armour. And there needed to be more convenient ways for people to access these benefits online. But at the same time, if you'll recall, there was this notion of Stolen Valor going on where a lot of people were fraudulently claiming to have served in order to take advantage of of these businesses that we're trying to do something special for members of military. So I got into identity specifically to solve that problem of how do we help members of the military and their families access benefits and services online? And how do we protect those businesses in what became government agencies as well from you know, fraud and abuse of these programs from people that were fraudulently claiming to serve but, you know, quickly learned that the problem was much bigger than just the military community, really, all of us struggle, John, to prove our identity online. And that problem has only gotten harder and more pronounced over the past 10 to 12 years that I've been in this space. So I went from CO founding what became it me to leading a team for the consumer identity organization at Capital One. So I worked within banking, you know, to really solve for identity verification and fraud. It's AOL tremendous scale, in a and understood a lot of the regulations that banks and financial services were subjected to. And then from there I, I spent several years

leading the identity business for a company you may have never heard of called idemia. But is, is likely in your wallet in the form of a driver's license or a credit card. And you may have seen idemia, as you've come through the precheck process for TSA, or as you've gone through a security checkpoint, I know, you know, we're not traveling as much now. But next time you go through an airport, you'll probably CIMB has brand, they're verifying your driver's license or passport, at the checkpoint to make sure, you know that we're only letting people through who are legitimate. And so I worked in that space for for several years, leading identity identity as business during the pandemic, though, you know, I saw a lot of my state and federal partners, really struggling to digitize their services to distribute benefits their digital channels and being taken advantage of, by very sophisticated fraud rings that were organized, and in manipulating a lot of the benefit programs. And I, you know, I'd seen a lot of this before, in my time at Capital One and knew a lot of the technologies that were necessary to solve it. And, you know, I like to be, you know, in a place to be able to help my partner solve their problems. And we just didn't have a complete toolkit for doing that at idemia. So, you know, I started to partner with so cure at the time, brought them into some government opportunities, and, you know, really got to test out their platform as a partner with some government customers, before making the transition. And talking with the CEO of secure Johnny Aris about the importance for solving this problem in government, or civic duty to do that. Yeah,



07:03
I want to s o cure.com. Look at the founders, quite an international group there, you know, Brazilians and people from me, sisters, it's a mix and match of everyone, because I think this is not just an American problem, it's a problem everywhere, isn't it?

07:16
It is a problem everywhere. And just quickly on the founding story of the company, which I think is interesting and relevant, again, for your audience here, especially in government. So the company was started by a millennial and someone who was new to country, neither of whom could open a bank account online. And largely, because a lot of the traditional ways that banks were using at the time, you know, we're not able to resolve their identity information, because they didn't have credit files. And so, you know, there's a large part of the population that have what's called thin credit files, or no credit files, or who are new to country and kind of invisible within that system, you know, but still need ways to prove their identity. So Johnny and his partner went to work on really solving for how do we verify these hard to verify populations. And they started with a machine learning data science first approach, you know, which is now much more, you know, the fad, if you will, and something that everyone is claiming to do, but, you know, they started way before it was cool. And by having, you know, that 10 plus year, you know, experience and learning, you know, they in that start with, how do we verify people who are new to country, people who are thin filed no credit file, and how to help verify them, they've become the most accurate and built the most accurate and inclusive, identity verification, fraud prevention platform in the US. So to highlight that piece, because

08:59
so your personal story and your corporate story, both are problem solution. So this isn't build a pair of shoes and try to sell them on K Street. It was, hey, this is a problem. You know, it's raining, we're gonna have waterproof shoes. So that's, that's reassuring. I went to your LinkedIn profile. And I saw something called a

cantar initiative. And with your background, I thought that was martial arts or sword fighting or whatever you do in your spare time. So what is this Kantara initiative?

09:27

Yeah, so I've been engaged with the cancer initiative for the past decade. Cantera is really the the leading standards and best practices organization for identity globally. And as you rightly pointed out, this is a global challenge. You know, there's been a lot of studies on you know, digital inclusion and the impact that has on economies around the world. But But cancer initiative has been working to advance standards in the area of is really individual or citizen identity access, and to collaborate and innovate and build best practices, user managed access is one of the things that you may have heard of that's come come out of this. And, you know, we really have a focus on enabling clear, inequitable exchange of value for personal data and information and the protection of that data by you know, the people that are entrusted with it. And identity is really critical infrastructure, you know, for enabling trust in in American society and more broadly around the world. And so, you know, we really believe in the importance of getting that right, and doing that equitably and transparently.



10:50

So let me, let me paint the picture for the audience for about 60% of the audience are Garvey's okay. And so they may do some research. And they find out that, you know, companies started in 2012. Apparently, all the big dogs, all the big banks are using you guys. That's right. I mean, I mean, if you look at your website, it's like, well, who isn't using, it seems like it's very, very pervasive. And so we have a situation, the federal government, where COVID comes in accelerating digital transformation, all of a sudden, here we go. Problem Solution. Again, we have situations where there may be people perpetrating fraud, there may be a lot of money available from the government that's not being allocated, how's this for discrete not being allocated appropriately? And, and then all of a sudden, we have Matt Thompson launching a federal initiative and saying, Hey, we've done it with all the big dogs. I mean, I've worked at a bank. I mean, if you've got trust, you know, if there's anyone in my podcast history that has trust on his forehead is, hey, been there, done that got the t shirt been beat up, knocked around? Banking. And so, I mean, I think you should have pretty good credibility, no matter

11:57

what I, I appreciate that. And I just want to correct one thing you said, it's not there may be there, there definitively is massive amounts of access issues in terms of, you know, good people not being able to get easy access to their benefits. And unfortunately, a lot of what we saw were, you know, people who were in most need of benefits, you know, not being able to easily prove their identity to access those and being subjected to extremely long wait times to get access to those benefits, or having to go through a whole lot of friction. And on the flip side of that, seeing a lot of fraud and, you know, I read a lot of the reports, obviously, I have to, to understand kind of the the industry and the trends, but um, you know, if you if you read the reports that were published, FBI, Secret Service, etc. You know, there, there's a lot of references to organized fraud rings that were manipulating these benefits. And, you know, there are a lot of estimates out there. You know, but I think it's safe to say, well over $100 billion went out fraudulently, during the pandemic. And, yeah, I mean, I think back to what you were saying earlier. So cure is really the premier kind of identity verification fraud prevention platform being used by for the top five banks 13 of the top 15, credit card issuers, every major FinTech, which

is really where the company got its start, crypto exchanges, online gaming. You know, we we span a number of industries. And we're now live today in both California and Florida, producing commensurate results which are best in class results, empirically. Meaning I like to prove all this stuff with data, not just marketing speak, and that's one of the things that I'd love is a call to action for your federal audiences is go test this stuff. You know, I think, you know, two things. One, during the pandemic, people had to make quick decisions with limited information, which is what leaders have to do. I mean, again, that was kind of the common operating model when you were in combat. You know, and this was a crisis situation and, you know, they're, they're needed to be quick decisions made to move solutions in place to enable, you know, this from being, you know, to stop it from being a free for all. So, things were done, and I think appropriately done during the pandemic, but but there's an opportunity now, to fix a lot of the problems that we saw happen with a lot of what was done quickly during the pandemic and more time to really test out different solutions. and do more market evaluation than, you know, procure using emergency authorizations and kind of move more quickly than probably many were comfortable doing to, to implement solutions during the pandemic. So, you know, we're really pushing for government leaders to, to do more market research on identity verification fraud, which was something that a lot of them knew little to nothing about at the beginning of the pandemic, and then became very, you know, came a top priority because it's so central to enabling digital transformation.



15:35

But look, I think, John, it's important that, you know, we don't kind of accept the status quo as being representative of what good looks like when it comes to identity, and fraud, verification and government, there is better betters being used in in financial services, probably because they're further down this digital transformation path, they've been dealing with fraud at scale, much longer and a much bigger scale than then the government has seen until recently, through digital channels. And, you know, I think at the end of the day, there's a lot of best practices that can be gleaned from financial services, but a lot of improvement that can be also understood through through testing of solutions. But one of the things that makes me cringe a little bit, John, when I'm engaging with government leaders is this notion that fraud, that they have fraud under control that it's solved, fraud is a constantly evolving thing. And the next pandemic is right around the corner may not be a health related one, but you know, there's a high likelihood of a financial one, that's not my area of expertise anymore. You know, but at the end of the day, you know, the next pandemic, the next economic crisis, whatever is around the corner, and we need to prepare now for that, and we need to do it in government to make sure that we don't have the same kind of access issues that we saw during the pandemic, or the fraud problems, because both of those problems are only getting

17:03

harder. I'm gonna paint a commercial picture and CFS application the federal government, if, if I want to buy a pair of shoes, and I go to Matthews, shoe store.com and takes me forever to find the stupid shoe I'm about usually it's three seconds. Now if I go to Gilroy shoes, and it's real fast, hey, and I'm gonna buy those shoes for my next to triathlon. So in the marketing world, that's called friction. And when you go online for the federal job to get information, whether it's medical information, whether it's tax information, I think reducing friction is going to get better customer buyers, and I think it's going to improve service that and in case you haven't noticed it, the federal government's coming in more and more initiatives on improving customer citizen experience, and

so just swapped customer for citizen and, and that's what your technology allows, because the machine learning to speeds it up, doesn't it?

17:59

It does, it does. And, you know, I plan a lot of the efforts, and I'm working with a lot of the mission owners in both federal and state that are really taking the executive order on customer experience and initiatives around customer experience to heart and working on how they improve that because, you know, I think there's broad recognition that there's a lot of opportunity to improve in that area. You know, I came from the business, as I mentioned, that supported a lot of the DMVs. And, you know, DMV is not usually regarded as, you know, a great experience people, you know, have to go and wait usually, most of the day, if not all days in some states, and you know, and there's a push within the DMV community to get people out of the office and engage with them anywhere at any time, so that they don't have to dedicate a day to to showing up somewhere. You're seeing that across all of government in terms of thinking through how to better enable access, kind of from an anywhere anytime approach through any channel, which really increases the emphasis on how do I verify that the person at the other end of this transaction is who that person claims to be? You know, and is a real person. And those questions have gotten dramatically harder to answer over the past decade. Really, because all of our data, John, your your data, my data, everybody's data has been compromised now multiple times over through these large data breaches. And so and fraudsters have really democratized a lot of sophisticated tools. So, you know, people who are kind of novices at fraud are able to network well within the fraud community access of best practices that are shared tactics, techniques, procedures that are promoted for how to defeat different commercial entities controls and government controls. And, you know, you see step by step guides on what to do. And, you know, you mentioned machine learning, which is at the core of what soak your does to provide that better customer experience, more accurate results. But at the same time, we're seeing fraudsters use a lot of AI. And so, you know, if if government agencies aren't using machine learning against that kind of more advanced attacks, there's going to be challenges, there's going to be challenges I went



20:45

to so cure.com, this morning, read a few blog posts watched a few webinars, and there's a phrase that popped up called synthetic identity fraud. Maybe you could define that for me, because it's gotten me kind of flustered.

20:59

Sure, and it's certainly a type of fraud that has become much more prevalent over the last decade, you know, we started to see it rise pretty quickly and dramatically within, you know, credit card companies, financial institutions, and we are starting to see it now as well in government benefits. So, and we've built specific controls, and algorithms to help combat from synthetic identity fraud. But effectively, the easiest way, I think, to understand this is like a Frankenstein identity that takes combinations of of different real identity elements, combines those, you know, and then builds up, you know, a profile over time, you know, that that largely is able to be used, you know, to to perpetrate fraud, and get through a lot of, you know, these points solutions, these rules based approach is that don't look at identity holistically, but look at individual elements of an identity. And when you just look at an identity, individual element of identity, say, you know, is this a real phone number is this phone number associated with this first and last name, you know, you're just seeing a small

narrow view of the identity and synthetic fraudsters are able to manipulate that by, you know, using real elements in combination together, you know, to create a fake identity.

22:39
Johnny Ayers, a founder of your company was on YouTube. And then he he mentioned this phrase called an ID graph. And I think this is a maybe a patent or proprietary application that you have, and I, I immediately want to go to the whiteboard. And okay, what's this mean? And so, so what is the what is an ID graph anyway?



22:55
Yeah, so, um, you know, so cure takes a very different approach to solving for identity verification and fraud prevention, then I've seen in the market, and this is kind of the singular area I've been focused on for my sieving career. You know, the identity graph effectively, is analyzing all of the kinds of digital breadcrumbs that you that you use across a network of different digital engagements that you have. It's, it's reinforced within our model by feedback data that we get from, from our customer base. So our customers and one of the things that is relatively unique to secure is that we're getting and have built up over a billion rows now of feedback data, where every time we process a transaction, that entity, whether it's a credit card information, credit card company or bank will say, Yes, this ended up being a good identity, or there was fraud associated with this and basically validating, confirming that the identity information that we verified was, in fact, true to the, the output that we produced the recommendation that we made. And so not only are we analyzing kind of this, this digital footprint, and elements of that, you know, to really provide more predictive power in terms of how we get to accurately identifying someone is good or bad in the future. You know, but it's really kind of stitching together, our customer base and leveraging feedback that we're getting and where we're seeing, you know, identity profiles kind of being built in trust grow over time, as we are able to analyze kind of more data. You know, the other piece of that is is really in the ability to also see fraud patterns. So by building the identity graph, we also see fraud patterns evolve over a network. And I really think this networked approach to combating identity fraud is the right approach and the best approach because as I mentioned a little bit ago, fraudsters are really networks. And we've got to be better networked in terms of signals and information that we're using to vet a good versus bad identity.

25:36
Well, Matthew, you're a well educated gentleman. And so I'm going to use a quotation from a philosopher, that's been impressive. And the philosopher I want to use his guy name, Yogi Berra. Berra said, The future ain't what it used to be. And so, so look into your crystal ball there, and you do a lot of predictive things with your company. So you're, you know, because I, I'm an old guy, I've been beat up. And I think there has to be some kind of an event that's going to force someone to start going to the gym, or for someone to balance their checkbook, or whatever it happens to be. And so So where do you see the next five to eight years heading as far as identity management, zero trust this whole digital transformation?

26:17
Yeah, and we didn't get too much into zero trust, but one, great initiative, it's a great strategy that has really elevated, you know, the cyber awareness and profile, you know, in tools, etc. By the way, identity is the first

pillar within the zero trust strategy. But, you know, I would say, I would say, I think we had an event, and that event was COVID. And I think, you know, that event, and it's opportunities like this, John, with with your audience to raise kind of the awareness and understanding of the critical role that identity plays, enabling access to benefits and enabling trust in our society. And I think it's becoming more in the forefront. It's raising as a priority. Certainly, among the state CIO population, I just had the benefit of attending NASCIO and engaging with a lot of state CIOs, where identity, you know, access management was one of their top three initiatives. And, you know, I'm seeing similar focus on the federal level as well. And so I think the profile has risen. I think we're starting to see, you know, executive orders and policy being developed, I think we're seeing mission owners within government get more involved and knowledgeable about identity, and and how it's done right and educated. I think we still got a long way to go in terms of educating, which is why again, this speaking with your audience, and you today is so important to me, you know, because we really want to lay the foundation here in building blocks for for how to do this, right. But I think we've had that event, I think you're going to see, you know, more government stepping into play more of a role going forward in terms of, you know, providing digital identity solutions for citizens or the general public, we're starting to see that and one of the areas I worked very, very heavily on was mobile driver's license, I think that will be something over the next horizon that you mentioned, five to seven years, that is a major game changer in this space. I think you'll see other government authoritative data bases kind of open up to verify elements of of the public's identity, again, hopefully doing it under, you know, user managed access and controls, and with transparency, and permission by the individual whose identity and permissions associated with that. But at the end of day, I think you'll see government stepping up in a much bigger way over the next five to seven years. And I think you'll you'll see the implementation and the usage of more advanced methods of verifying identity enabling access, preventing fraud, by the implementation of technology platforms, like so pure, and others, and we're not the only you know, we do what we do, you know, empirically better than anyone else, but we don't do it all as well. And so, you know, and I don't think anyone should believe anyone that comes in and says they do it all, especially not in the identity space. It's a very fragmented industry, which, which has also made it harder for government mission owners to really kind of get their arms around how all this stuff works together. But at the end of the day, I think we've had the event I think you're gonna see increased policy funding initiatives. And as I mentioned earlier on, and I'll continue to reinforce, I hope, more testing. And I hope to see NIST play a bigger role. Because that is something that they're known to do is testing here with identity verification technologies and providing transparency around performance so that government leaders can go in more informed, you know, and not be kind of misled to believe that 70% is a good performance benchmark.



30:36

Gotta use that model for the license plates. And Missouri has shown me that's, that's awesome for this interview. Is that really, okay, is it fast? Let's try it and test it out. And I think that's what you said, between the lines. Good, good, good. That's exactly what I said. And hopefully it wasn't between the lines. I was trying. But yeah, well, we're running out of time on Friday. We could do you know, I could probably do Identity Management podcast weekly. And so many aspects of it. I mean, just driver's license artist identity with mobile devices. I mean, it's a whole. It's a huge world, way bigger than I ever imagined it was. It's great. Well, unfortunately, we're running out of time here. You've been listening to the federal tech podcast with John Gilroy. I'd like to thank my guest, Matt Thompson, General Manager of Public Sector solutions at so cure. Thank you, Matt.

that. But thanks so much. This was awesome. Bye bye.