HOMELAND SECURITY EXPERTS GROUP (HSEG)

2022 HOMELAND SECURITY ENTERPRISE FORUM

LIGHTNING ROUND 3:

FUTURE OF BIOMETRIC IDENTITY

Salamander Resort & Spa

Middleburg, Virginia

Wednesday, October 26, 2022

Lightning Round 3 - Future of Biometric Identity

MR. PISTOLE: It's my privilege and honor this morning to do a lightning round with Caryn Seidman-Becker, who is the co-founder, with Caryn is back here someplace, yeah, co-founder of -- we know, it's CLEAR back in 2010. And Caryn is known as an innovator, an entrepreneur, an investor, a motivator, and a leader. And so, she's taken this company with again to make it into something that is, I don't want to say ubiquitous, but in over almost 15 (cross talk) now.

MS. SEIDMAN-BECKER: Working on it, yeah, yeah.

MR. PISTOLE: And over 15 or so professional sports arenas --

MS. SEIDMAN-BECKER: Yeah.

MR. PISTOLE: -- around the country. And so, what just a few questions about identity management, verification, how does that work, how does that help improve security as opposed to having long queues, which could be a terrorist target, as well, you know.

So Caryn, if we can just start off, lots of other things to say about her, but we may have time for one or two questions, depending on how long we go. So, tell us about in terms of CLEAR what is your goal, your motivation? And how do you go about accomplishing that?

MS. SEIDMAN-BECKER: Yeah. And so, let me also start by saying thank you to you. In 2012, when you launched precheck, you really brought risk-based screening and identity-based screening, two checkpoints, and I think permanently transformed the trajectory of airport security. So, I want to say a big thank you to you.

(Applause)

MR. PISTOLE: Thank you.

MS. SEIDMAN-BECKER: The beginning motivation before we ever get to biometrics was to make experiences safer and easier. 911 had an impact on me and my life. And the ability to be part of the solution on behalf of American travelers, was really the motivation. I started on Wall Street and as I said, I didn't want to die and have people say I pick good stocks, I wanted to build something that made the world a better place. My parents both worked for the government. I grew up here in Maryland. That was the beginning motivation.

And we're working on it every day. We now have over 3,200 team members who are making it happen. And it's rooted in biometrics, right? And so, biometrics are about building an impermeable link between you and your unique characteristics, face, fingerprint, eyes, voice. And there's more coming. People talk about gait and also -- G-a-i-t and all sorts of other things.

And you know, without the ability that technology was undeveloped 50 years ago to use biometrics, we took to using plastic cards to assert identity, who we are and what we should have access to. And in a post-911 environment, there were these tradeoffs between making experiences safer or easier, right? That which made it safer, created longer lines or more difficult experiences, and that which made it easier or what we call frictionless at CLEAR, made it less safe.

And we saw biometrics as the end, making it safer and easier. It was used in the military in 2010, when we started CLEAR. It was used in Brazil for voting 13 years ago, some thoughts here for the U.S. And it was used in Asia for financial services. And so, we really believed in the consumerization of biometrics in the U.S., and have gone about building an interoperable biometric identity platform where you can enroll once, and then assert your identity in multiple use cases. And today, we have well over 14 million Americans on the platform and using it. And so, the motivation is every day when people say they love CLEAR, they trust CLEAR, and it changes their lives.

MR. PISTOLE: Yeah. Thank you for that overview. So, you mentioned biometrics, that's what drives the company, the policies, procedures, protocols. How are biometrics more secure than what we all know? We no longer passwords you can do all that. There's ways of doing it. So, just tell us briefly about that?

MS. SEIDMAN-BECKER: Right. It's sort of interesting, I use one password, and I look and I have 146 passwords in there, which by the way I unlock with my face, right? So, it's interesting. But you're using these pins to assert your identity, who you are and what you should have access to, whether it be logging on to Okta (phonetic) or your New York Times account. And so, you know, is that the safest way?

And we believe identity is connecting you to all the things that make you, you. ID is one piece of that, but not only the cards in your wallet, but also your attributes and insights. And I think in a post COVID environment where the world has gotten more digital, far faster than I think anyone expected; security, trust, and identity are foundational. You read articles of late about LinkedIn. And it's an epidemic. People are impersonating. You know, many people and so there's a whole article about CISOs. And people are real picture, totally fake job. And then, there's people writing, you know, that's one of the top 50 CISOs because someone said they were the CISO at Coca Cola.

And so, it's really about building this interoperable system connecting you to all your attributes and insights. I'm always me, but I'm one person when I show up at the hospital. I'm Caryn on my health care insurance, on my eligibility on my copay, and my electronic health records. I'm still Caryn when I show up at the airport and on my driver's license, my boarding pass, my frequent flyer number, my pre-check status, whatever the case may be.

And so, the ability to connect you is actually safer and easier from a security perspective, because we started as a public-private partnership with the Department of Homeland Security 13 years ago, we're FISMA high for multi-layered system in GovCloud. And so, it's about building this very secure system.

But I also believe that people are oversharing today. So, when you hand someone a plastic card or driver's license, there's a lot of PII on that. They just need to see that you're over 21, right? If you're doing something that you need to be over 21 on.

And so, all they need to know is your Caryn Seidman-Becker and I'm over 21. And so, I really believe that biometrics are safer and more frictionless than the 13 user passcode, 10 happens to have a Coinbase account. And he's constantly telling me that he gets locked out because he can't remember the 12 unit password. So, he's, you know, having to retake a picture of his driver's license and reassert his identity, right? That's not optimal. On multiple use cases, you have a drop off of conversion, you have less security. And so, I clearly believe biometrics are the future. And I think the future is here.

MR. PISTOLE: So, you talk about that the ability to use biometrics, those individual unique identifiers for each person. What does CLEAR do in terms of preserving and securing that database from all these hacks out there? All these -- (Cross talk)

MS. SEIDMAN-BECKER: Yeah. Absolutely. You know, because we started in aviation and because we started in a public-private partnership, security has been job one from day one. And both how we've constructed the system and architected this system from a multi-layer perspective and then, the different, right, requirements that have gone on from FISMA High, which wasn't there, right, a decade ago. And we met the data being in GovCloud.

But also, you want to serve partners where they want to be served. That could be on the Cloud, that could be on the phone, longer-term that could be on chain. Also, when you think about it multi-factor authentication, right? So, sometimes maybe face is good enough, but sometimes it's face and voice, sometimes it's fingerprints and iris. And so, different use cases require different biometrics or different permutations. Right? So, if you or your face is your ticket to get into the Yankees game or to buy a beer, it's very different than getting on an airplane.

And so, constructing a system and again, I also think from a culture perspective because we started with just me and Ken in a room in 2010 and now have 3,200 team members across the country. It's really about your culture and your leadership, and how you construct it, and how you partner.

MR. PISTOLE: So, I'm just curious if you are a member of CLEAR or you know somebody who is? Just show a hand, if any. So, there's, yeah. So probably get some testimonial, hopefully positive. We won't do that right now.

MS. SEIDMAN-BECKER: Not enough. But that's opportunity.

MR. PISTOLE: Yeah, it's opportunity. So, one of the keys is -- one of the keys, in terms of CLEAR providing the expedited queue at the TSA checkpoint it's not the security, the physical security, it's the information security that helps inform TSA as to whether known and trusted travel, but this person who shows up is a person who's purporting to be that person on boarding pass and all that. So, it is a public-private partnership.

What do you say to those people say well, that's fine, but it's still not the physical security that TSA has to do? What's the partnership there?

MS. SEIDMAN-BECKER: Right. Look, I think TSA owns the physical screening a 100 percent. But you have to actually pull back for a minute. When somebody's journey begins, it begins when they book a ticket. It begins the day of travel when they leave their house. And so, building multiple use cases along that chain, it's not just the airport security checkpoint. And so, you want to build a system that when I go back to interoperable, interoperable with TSA that we can tell TSA, this is Caryn Seidman Becker, what they want to do with it, but we already have 14.5 million people on the platform who have already enrolled. Do you want to be able to say this is Caryn side Becker? Assuming Caryn Simon Becker, of course opts in for that.

And then, you want to go back though, because there's backdrop, right, which creates lines, there's lounge access, there's boarding, there's concessions. We have something on a mobile app called Home to Gate, it tells you when to leave your house, to get to your gate 40 minutes to go because we've mapped out the travel, the airport security lane, and then we've mapped the walk from the security lane to your gate. Right?

It's about putting it all together. And TSA is responsible, right, for physical screening. And I think our public-private partnership and we have innovation partnerships going with them about how you work together to drive innovation further and faster, but we fully respect what the Department of Homeland Security has to do. And I think it's with that respect and that innovation that you work together.

MR. PISTOLE: So --

MS. SEIDMAN-BECKER: I acknowledge the challenge of public-private partnership.

MR. PISTOLE: Yeah, yeah. So, last question I have and then I think we'll have time to take one or two questions. So, the future biometrics writ large and what is the checkpoint of the future look like from your perspective?

MS. SEIDMAN-BECKER: You know, I think you see the checkpoint of future in places outside the U.S., right? A lot of automation and a lot of technology. So, I was in Dubai, you know, in December and there's eGates. In Asia, there's eGates. There's facial to get into. In Kenya, you, you know, use biometrics there. And so, I think that biometrics from curb to gate, backdrop to boarding, never having to take your wallet out of your pocket is absolutely the future. And I think on behalf of American travelers who have had really challenged experiences over the past year, I mean, we talked about this, if you are 2.5 million today, how are you going to scale that experience to 3 million to 4 million?

I also think there's opportunities for remote network monitoring, right? So, I think you can make it safer and easier. I think it can benefit airlines, because more people will travel, they'll get on planes happier. I think that net promoter score customer happiness is something we're obsessed with, as well as security. And when people are happy, they will travel more. And those are good things.

And so, I really -- I also think, you know, how do you have screening off site and that there's all sorts of things sterile buses, landside, there's so many opportunities. And I do believe that it's not just the biometrics piece, right, but the hardware piece and making sure it's interoperable.

And so, I think it's a really exciting challenge time and travel, but that dh from crisis comes opportunity. And I think, you know, the travel industry has had 911, then it had the downturn of 2008, 2009, then it had the pandemic. And it's like every 10 years there's another challenge and we have to invest for the future and we have to invest together.

In an airport, there's the airport employees, the airline employees, the TSA employees, sometimes the police or the fire department depending upon, and you really need people working together on behalf of American travelers to make it safer and easier. And so, we're excited to play, you know, to play a role in that.

MR. PISTOLE: Good. You're open to take a couple of questions?

MS. SEIDMAN-BECKER: Sure.

MR. PISTOLE: So, questions? There's microphone.

UNIDENTIFIED SPEAKER: John, right here. I'm sorry, Jane. So, Caryn, two things real quick. How do you address -- last night we hosted a debate on misinformation. How do you address the misinformation about biometric, biases, and issues in that? And number 2, you're collecting a lot of PII data, how secure is it? What are you doing with it, et cetera?

MS. SEIDMAN-BECKER: Yeah. So, first of all, something that I have been very transparent on from the beginning, because we started with fingerprints and eyes is that there is racial bias and facial recognition. And that is something that the industry is working on. And I think massive improvements have been made. But to not say that, I think is dishonest. And I think, you know, we've built a lot of technology to help them. It's something we continue to work on. But you know, through lights, and you see the new Google Camera that they talk about on their phone, the industry is addressing it. But I think you have to be transparent about it, number 1.

Number 2, there's two points. There's privacy and there's data security, right? And so, from a privacy perspective, we've always said we do not sell share or rent data, right? We have said that everything we do is opt-in. And that's really important both in the U.S., as you see the U.S. privacy laws in California and BIPA in Illinois, but also internationally with GDPR, et cetera. And so, we've always built a system that is compliant from a privacy perspective.

And again, when we talk about data security and a multi-layered approach and starting in aviation, I would say, we didn't start with buying bottled water at the corner deli, right? And saying, oh, yeah, you know, it's good enough. We started here in aviation security, where there was a regulatory environment, right? We started in a public-private partnership with the Department of Homeland Security and our system has been constructed accordingly.

UNIDENTIFIED SPEAKER: Caryn, congratulations on your success. It's a huge, great company. And everyone here is impressed. Certainly, I'm impressed. But it's I wanted to ask a related question to whatever his name is just asked you, I forget his name.

MR. PISTOLE: That one there.

UNIDENTIFIED SPEAKER: And that is, you've made it clear that people opt-in. And if they don't want to be part of it, they don't have to be part of it. But as you build an international network, aren't you kind of stuck with lower standards, possibly in other countries? And what about travelers who go to China? Let's just pick a random country, China. And how secure is your impressive database when they land in China? And --

MS. SEIDMAN-BECKER: We're not -- that's --

UNIDENTIFIED SPEAKER: -- whatever they have on their devices?

MS. SEIDMAN-BECKER: Yes. So, I think that's a really important piece, which is today we are not in China or Russia or places like that. And we made it -- I think I started with as a mother of three, I had no desire to fly there. So, that was sort of off the table. And then, it became a data security issue.

And so, the answer is that, you know, if something's in the Cloud, it's in our Cloud here in the U.S. on GovCloud, where CIA data is and there's no access over there, we're not even over there. And so, also as a FISMA high company, not only do all the components have to be, right, within regulatory spec, and nothing from China, but the employees who touch the equipment have to be. And the data on the phone is on the phone and encrypted and from a face perspective, is just simply that.

And so, whether by luck or by skill, we're not over there and everything we do is encrypted and rest encrypted at transit and yeah.

MR. PISTOLE: So, I think you'll be around for least a little bit after this session --

MS. SEIDMAN-BECKER: Yeah.

MR. PISTOLE: -- and after the next session, during the break or something. So, let's give a warm thanks to Caryn Seidman-Becker.

(Applause)

\* \* \* \* \*