Journey and their Comprehensive Trusted Identity Platform

Journey and their Comprehensive Trusted Identity Platform

Presented By: CrmXchange

The internet was created without an identity layer because it was intended to be a free exchange of information. But now billions of transactions take place daily that are very sensitive in nature, from online banking to applying for mortgages to paying your taxes. Establishing trusted digital identity is absolutely crucial to protecting those interactions, but until recently solving the digital identity challenge required unpleasant tradeoffs between fraud and friction on the customer experience. Led by an entrepreneurial team offering vast contact center experience, digital engagement innovation, and engineering expertise, Journey has created a comprehensive Trusted Identity Platform. The goal is to totally transform the complex process of identity verification and customer authentication. The company employs what they call a "Zero Knowledge" network-based approach. This cryptographic concept enables individuals to prove they are exactly who they say they are without exposing sensitive details to fraudsters.

In her continuing series of interviews with solution providers that had planned to exhibit at postponed industry events, CrmXchange Managing Partner, Sheri Greenhaus, conducted an in-depth conversation with Journey's CEO Brett Shockley and President Alex Shockley.

Origins and overview:

Alex Shockley: I ran a digital strategy for a creative agency called Shocking Creations that was sold to a much larger ad agency in Denver called AOR. I was tasked with learning how to find our best prospects, have them engage with the digital content and measure what is happening across the customer lifecycle through the various optimization campaigns. It's a little bit of advertising, a little social media and use of analytics on the UI/UX theory.

Our co-founder and my father, Brett Shockley, had left Avaya and was serving on company boards. We'd been having ongoing conversations about the fact that while we were operating separately, we were two sides of the same coin. In my world, it was 'how do you find people on digital channels and influence their journey while they are tied to an anonymous identifier?' We don't know exactly who the person navigating through a web is, but we can begin to amass details about which browsers they are using and in what sessions they are taking part. We can see what they have and have not engaged. As soon as they pick up the phone to talk to the company and purchase the product, I equate that to the finish line. But for someone in the world of communications like Brett, it's just the starting line. We originally founded our company on the impetus of wanting to create a journey orchestration engine to inspire better designs to service the totality of the customer lifecycle. That is where the name Journey.Ai came from.

Journey and their Comprehensive Trusted Identity Platform

We've pivoted a bit since then. As we started going down these different pathways, we built different prototypes. We bumped into Cambridge Analytica on the marketing and analytics side. On the communications side, we saw what companies such as Affiniti and Mattersight were doing. We realized we were operating in an environment where companies took advantage of customer information without it being a win-win proposition for the customer and the business alike. At the time, we saw what looked like a brick wall for these companies coming from privacy regulations as well as from security and user experience (UX) issues. We figured out at the crux of this was the ability to cross over from being an anonymous identifier to a known person. At some point, the business has to determine who they are interacting with. All the cautions…security, UX and digital privacy… boil down to being able to understand who the person they are dealing with really is.

About two years ago, we focused on solving the digital identity problem as the root of trust in this customer lifecycle ecosystem. How does the business help the customer in establishing stronger proof that they are who they say they are? How does the company make it easier for customers to demonstrate that in a way that resolves all these issues as opposed to treating them as a tradeoff between security, privacy and UX? How do we protect the network of who gains access to what at any given time without proliferating copy-and-paste databases: these massive data lakes of every piece of customer information that a company can obtain. This practice can lead to data breaches. We sought to find a way to re-orchestrate this from the network up to develop a better customer lifecycle and create a suite of solutions all along this lifecycle.

Solving the digital identity challenge

Brett Shockley: We are doing one thing very differently. We reached the conclusion that if you can put verified identity at the root of trust in the relationship between the consumer and the business, then all these applications get dramatically easier and a lot more effective. That was the starting point. Then we looked at how to actually accomplish that goal and took more of a network-based approach. If you look at our industry, what you see historically over the past 30 years are a series of point products that have been cobbled together to do what needs to be done. But this approach leads to solutions with lots of holes. People have become accustomed to it because their companies have grown up with it. But we all know how complicated we've made it when we try to hire someone new into the industry. It takes forever to explain what it's all about.

Underneath our network approach is the Zero Knowledge Identity Network. The concept behind it wasn't simply to come up with another point product that did authentication or obscured customer data in a credit card transaction or allowed someone to sign off on a document during a phone interaction. Our intent was to find a way to make all these functions work more easily and effectively. We have a whole new set of technology tools that weren't available even two or three years ago. Of course, we all now carry around smartphones that have sophisticated sensor technology that helps makes these additional capabilities possible.

Journey and their Comprehensive Trusted Identity Platform

When we looked at it holistically through the eyes of the customer, we realized we could change the nature of the game. How do individuals sign up for new accounts while getting their identity verified? How can someone be authenticated before interacting with a company? More important, how can that be done with at one-in-a billion veracity reliability where many products today are only operating in the 65% (with knowledgebase identification) to 94% range (with voice base identification). Verifying one factor is not enough. Businesses need to verify multiple factors. How does a business protect someone's privacy during all interactions and transactions while still allowing for the personalization they all want to deliver in an era that assigns such great importance to the customer experience? That's the philosophical approach that we've taken. I think it's exemplified in our slogan: "know your customer, not their mother's maiden name."

How it works

Alex Shockley: If you walk through the customer lifecycle, let's say someone wants to open a new account with a bank. The first thing they must do establish the person is who they say they are and is entitled to have an account. They have to go through a Banking Secrecy Act compliance 'know your customer' check. The bank will take the person's identity information and run it through a bunch of back-end databases to make sure they aren't on something like the terrorist watch list. That process today is full of holes and can take weeks to complete. Alex went to test this by opening an account at a Top Five US bank, whose pitch was to download their app, and everything will fall into place. It wound up taking almost five weeks.

In our solution, the agent desktop makes the process far easier. The customer can take a picture of a document such as their driver's license, both front and back, to confirm that it is readable and also allowing any bar code information to be scanned. The agent can then collect all the identity details, as well as take necessary steps to check the legitimacy of the document without exposing privacy. This meets the same standard threshold as having a teller at a bank accept the document in person. There is no 'Journey app,' but we have an SDK that sits within the existing mobile app of our enterprise clients which provides the ability to take these steps. The customer can then take a selfie which can be checked as matching the submitted photo ID. The solution can generate a 3D map of the face to be used for biometric identification later. The client can collect all the different identity details that the customer is claiming and take necessary steps determine the legitimacy of submitted documents. Journey encrypts all of that information within the device and sends that encrypted cyphertext to a suite provider where they can do the database checks to make sure the person applying is not on any watch, been convicted of money laundering or other financial crimes. When the individual passes that test, Journey generates a digital certificate which is then sent to the applicant's phone or to the bank, enabling the opening of the account. Depending on the quality and location origin of the document and the camera, this can be done in real time. If it is a US driver's license or passport, the sequence can be completed in about a minute, including getting the result. Even in a worst-case scenario, it can be done within a day. We can now support more applications from more than 180 nations with 4500 global identity documents.

Journey and their Comprehensive Trusted Identity Platform

The customer can then call into the bank. Journey turns the individual users' mobile app into an enriched source of truth in saying they are who they say they are. Beyond verifying the documents submitted, we're also equipping the user with multiple factors of biometric identification that they can then leverage for all subsequent interactions. This is the first point of differentiation in what we are enabling.

When a consumer calls into the contact center, they don't have to go through the process of keying in the 16-digit account number required or PIN or having to answer security questions as is required in many interactions. Statistically, fraudsters can often supply this information about 60% of the time. But when the phone number is registered, the contact center can do a check to see if there is a mobile app associated with it. If there is, the company can have the app or the IVR prompt the customer to log in through the mobile app to verify themselves and the agent. The agent can then answer the caller and address them by name, while providing their own authorization info. In the simplest form, what we're doing is connecting the app's authentication status into the contact center environment. It can be done with facial ID or through touch ID or its Android equivalent.

This is where we can use that second biometric element where a 3D scan of the face is generated. Facial ID had a one-in-a-million chance of fraud, where someone could pick up the user's phone and pass themselves off as the user. But the 3D ID and touch ID are only saved as templates on the phone, so if someone were to steal the device, they could theoretically re-register their face or thumbprint. Someone might do a sim swap or a phone porting attack and convinces the carrier to move the number to a different device, they could bypass those parameters. To solve for that, we are leveraging facial match. It can be deployed as running concurrently the face ID, so if you pass one, it automatically scans the second one. The company is then checking two different facial templates as well as two different live detection tests, so a potential fraudster couldn't get around it with any these tactics. These factors can be checked sequentially in as little as two seconds; contrast this with knowledgebase authentication, which is still used in about 92% of contact centers. Real users fail knowledgebase authentication about 32% of the time while fraudsters can pass about 60% of the time. Real users often fail to accurately key in their password, account number or PIN. We can get to about five to six 9s in accuracy within that two second timeframe. The only requirement for the user is to tap the notification on their device to identify themselves and the agent. It's a dramatic difference of the authentication sequence in the UX and security as well as in privacy. Once the user is authenticated, he can see the agent's name and identification number within their screen. We've borrowed this concept of mutual authentication largely from the ride sharing apps. By seeing who you are interacting with, it creates less anonymized transactions.

Giving the customer confidence in difficult situations

Brett Shockley: People often receive calls from banks or credit card companies which are reporting possible fraudulent actions. When they see "unknown caller" on their screen, they answer only about 15% of the time. And when they do answer in these situations, they are asked to answer identification questions which make them even more wary. It winds up that no more than 3-5% of the people give them the details they require to have a qualified conversation. A Tier One bank would launch over 500 million outbound calls in a year… just think about the wasted effort and frustration for both customers and the employees alike.

Journey and their Comprehensive Trusted Identity Platform

Alex Shockley: Our alternative is that since we have these integrations in the app and contact center, we can tie into the outbound dialer and predict when a customer's phone number is nearing the top of the outbound call queue. We can then programmatically push out an app-based notification to alert the customer of the need to have that conversation. It gives the customer the option of getting a call in the next 15 minutes or logging in to request a call at their convenience. The FBI recommends against using SMS to notify people of fraudulent activity for obvious reasons, but an app-based notification is totally different. It's far more secure and far harder to interrupt. Tapping on the notification also provides the choice of engaging in a chat session, scheduled at whatever time the business makes available.

There are three prongs in the process:

1. The first is notification to give the user a heads-up that there is a need to have a conversation and they will be receiving a call.
2. The second is the caller ID. Even if that number isn't saved in the users contact list, because we have the iteration with the outbound dialer as well as the mobile app, we can have dialer tell the mobile app to expect an incoming call moments before it arrives from a specific number coming out of a rotating pool of numbers. This rotating pool eliminates the opportunity to have someone spoof that number and call someone with it using the caller ID. It also allows us to pass contextual information to the app for the reason for that call. The customer will see X Bank, Fraud Dept. The mobile app is able to tell the caller ID what to display despite it not having been saved in the contact list.
3. The third prong is that when they answer the call---let's say the customer didn't' see the notification or the caller ID--rather than asking for sensitive information, they will say "Hi, This is Mary from X Bank: if you log in to the mobile app, you can see my agent information." It's that offer for a mutual exchange that produces far lower thresholds of anxiety than the security interrogations to which we're all accustomed.

If the agent asks for the customer's date of birth, for example, that information is entered on the app instead of being spoken aloud to the agent, who will only be told that it has been verified. No agent actually needs to know this information, just that the customer is supplying it correctly. This also applies to other sensitive information, such as social security numbers. The agent can once again find out that it's been verified through a zero knowledge query. This quite different from having to enter it on the dial pad and keying it in where it is stored as DTMF information in plain text.

In this case, we are bypassing the contact center entirely. We encrypt that information locally on the user's phone and send that cyphertext to the back end of the business where they can decrypt it against their records and send digital certificates using our technology, sending one to the agent and another to the user's phone. The agent can see the status and the user can see that the information passed, but it is never made available to anyone along that ecosystem. The zero knowledge cryptography allows the information to be send directly to the database to be checked. Rather than using a public private key exchange, the information has been obfuscated by an additional layer at the receiving end for the business's infrastructure. This uses what we call a Journey Identity Gateway where the data can be decrypted behind their firewall and fed to their APIs. It is never centralized with any other information. Since there is not centralized database where there are perhaps 500,00 records that can be accessed, hackers have far more limited opportunities. It also eliminates what we call a "man in the middle" attack, since the information is known only at both ends of the interaction. It's not worth it for a hacker, since even if they could break it, they would only receive one person's information.

Brett Shockley: By using the partner code we're showing to get it into their products, a client could literally implement Journey within a matter of hours. Of course, in a complex enterprise environment, it could take longer. It's quite different than the old days of CTI integration that could take forever.

Alex Shockley: In addition to doing text-based information, we can also securely take payments and take electronic document signatures. I find it extremely irritating when I am asked to verbally give account information which the agent could really give to anyone after the conversation. It is frustrating to know what they can jot down after the call or access from their screens. We use the same process to encrypt information within the phone and send it directly to the payment processor and once again, the agent never sees or hears any of it.

Who does Journey partner with?

Brett Shockley: Our partnerships fall into three categories. From a platform perspective, we are working with Cisco and Avaya right now. And to serve our clients, we are also working with a variety of other platforms. It's also contact center application providers, such as those creating dialers, CTI desktop applications or routing applications. We also partner with resellers and systems integrators. One of our partners in that area is Eventus, who works across many platforms. They have probably been the most active with their broad range of customers. Their client roster includes many BPOs which have struggled sending their agents to work from home because of privacy and PCI compliance for processing credit card numbers. We are working with their BPO customers around that specific issue to enable them to deal with Zero Knowledge, as it applies to home-based agents.

We've seen our solution integrated on Avaya, Cisco, Bright Pattern, NICE inContact, Amazon and Twilio. We've devoted a lot of time to making this easier from the UX perspective so that even if people are surprised by some of the capabilities, they are pleasantly surprised and were able to easily see what to do next. We did a lot of user testing across a variety of use cases. The goal with doing this in the network-based approach was to make it simple to do a broad spectrum of applications without having to do as many custom integrations as previous solutions required.

Journey and their Comprehensive Trusted Identity Platform

One early client was a trust company, whose customers set up IRAs of $50,00, $100,000, and more. It can routinely take four to five weeks to get that done with a couple of dozen phone calls, a bunch of electronic document signings and LexisNexis statements. We can accomplish this in five minutes with a higher degree of veracity. While it might not necessarily be a formal contact center application, it involves tying together all those functions to make it super-fast and easy, eliminating the need for all those phone calls to set up the account.

Alex Shockley: One important note from the consumer side is although it is apps-driven, we also have a browser-based solution as well. In this scenario, the user does not need to have a mobile app on their end and is can be a much lighter weight implementation on the agent side. With the browser-based piece, we can still facilitate Zero Knowledge interactions and transactions, including secure information transmission, payments, and e-signatures using the same cryptographic approach where those in the agent environment never see any raw data.

Brett Shockley: One of the most important things to get across is that companies should be looking at it through the eyes of the customer as they proceed through the customer journey. Our impetus was to perceive how easily and securely a customer could get signed up. We have talked about work-at-home agents, but even in the formal contact center, up until now, businesses have had to play all of these crazy games to turn the screen recording or voice recording on and off during sensitive information exchanges. They also had to transfer people to secure IVRs and take other measures to deal with privacy issues. We've made all that go away. In dealing with all the compliance issues associated with PCI, GDPR and HIPAA, we can allow all the transactions to happen securely without any of the contact center agents seeing the information. It's simply a fundamentally different approach in the way we have put the solution together.