Inbound Customer Authentication

Journey

Frictionless, Secure Customer Authentication Across Voice and Digital Channels

Almost every company still relies heavily on Knowledge Based Authentication, which is alarmingly ineffective, insecure, and irritating to users. KBA is a proxy for proving a person's identity by testing what they know, but this information is widely available to bad actors. It was created because the tools for exchanging information were limited to voice calls, dial pads, or keyboards.

But now, the vast majority of people around the world hold smartphones in their hands and have access to incredibly powerful sensors that create a new way of passing information back and forth, including cameras, touch screens, biometric sensors, location services, and more.

Contact Center Customer Authentication Across Channels

Journey has developed an award-winning and patented solution to establishing identity in the contact center with a unique network and platform approach that seamlessly blends biometrics and many other active and passive authentication techniques.

The magic lies in leveraging the sensors in a smartphone or laptop to capture inputs that prove a person's identity, not just what they know—using biometrics, document identification like a driver's license, biometric matching location, device and carrier data, past behaviors, and more. The multiplicative effect of combining identity proof points enables higher veracity of authentication for a high-value transaction.

If only basic authentication is needed, for example, to confirm an appointment, Journey has several options that are passive and frictionless, enabling you to get down to business immediately.

Key Benefits

1. Authenticate in less than 2 seconds
2. Completely passive authentication options available
3. Dramatically improve average handle time
4. Authentication travels through transfers
5. Facial biometric and proof of liveness cannot be stolen through social engineering
6. The contact center tech stack can be taken out of the scope of compliance
7. Invoke authentication from an agent desktop, IVR, IVA, Chat or any other system
8. Journey's Zero Knowledge Network® protects sensitive information and the security of corporate data
9. Flexible & agnostic - any desktop, any ACD, any channel, any data

Flexible Authentication Methods and Clients

To increase the security and privacy of the data exchange, Journey has built a platform and network to exchange information between the customer and agent or IVR, verifying it but not revealing it to anyone. This network and platform approach enables a considerable leap forward in security, privacy, and compliance posture.

Journey makes it easy to invoke a wide variety of authenticators from an agent, IVR, IVA or chatbot, including:

- an assortment of biometric authenticators (both active and passive voice, facial, liveness, fingerprint, behavioral),
- security questions via eForm (knowledge-based authenticator),
- device-based authenticators (username/password, FaceID, TouchID, location, etc.),
- browser-based authenticators (biometrics voice, facial, liveness, fingerprint, and location).

Secure, Privacy-Preserving Fraud Prevention

The Journey Trusted Identity Network is built on the principles of zero-knowledge cryptography and leverages the powerful sensors on smartphones, tablets, or laptops to create a modern and sleek customer experience for capturing biometrics or other inputs (like a finger signature, payment, or data capture on an eForm). Journey's advanced security techniques individually encrypt each session, verifying the requested data but only showing a pass or failure to the agent. With its ultra-secure architecture, even Journey cannot decrypt or store any transactions, providing the business with the most robust security, privacy, and data protection.

Requesting 2-factor authentication (2FA), multi-factor authentication, multi-factor biometric authentication, step-up, and mutual (agent and customer) authentications is also simple. All authentication validations follow the customer through transfers to improve the customer experience.

The network approach also plays a vital role in fraud prevention by aggregating the output of one or more authenticators to achieve the risk margin required for a given transaction. High veracity authentications, like facial biometrics plus liveness, provide high accuracy between 1 in 1 million False Acceptance Rate (FAR) with a less than 1% False Rejection Rate (FRR). Establishing a high veracity identity proof provides a solid fraud prevention measure. Fraud detection approaches include passive voice biometrics for continuous authentication and matching voice prints to known fraudster databases.

Authentication in its Many Flavors

Businesses handle authentication in a variety of ways. Some interactions don't require high veracity identity, but the riskiest ones need to be handled differently. Journey's authentication solutions are based on a platform and network approach, with low-code or no-code options for creating authentication flows.

Here's a quick overview of some options for authentication available from Journey.

Biometric Authentication

Over 90% of businesses today rely on Knowledge Based Authentication - usernames, passwords, silly "security" questions, which are distressingly easy to steal. Some add in irritating and time consuming additional checks like the Captcha liveness detection, or multi-factor authentication.

Biometrics, particularly ones that detect liveness, are not only simple and fast but also significantly more secure. Journey's approach enables various biometric options, including 3D facemaps, voice biometrics, behavioral biometrics, or device biometrics.

Advances in the sensors in mobile phones, tablets, and even laptops have enabled biometrics to verify and authenticate individuals for digital, phone, and in-person interactions. And Journey's approach adds additional security with our Zero Knowledge Network.

eForm and OCR

Journey can enable a zero knowledge exchange of information of almost any sort. A secure eForm can capture any information you want to authenticate (SSN, DOB, Address, account number, etc.). Customers can also use their camera to OCR a government ID, passport, payment card, or any document used to authenticate (such as a utility bill or a lease agreement).

Mutual Authentication

Mutual authentication is when both ends of the conversation have authenticated themselves. In most cases, the authentications will be shared between the two users.

In the case of the contact center, this is generally the agent and user exchanging identity credentials to create additional trust.

- Ideal for establishing mutual trust between two unknown parties
- Bolsters confidence in outbound calls, boosting right-party connect rates
- Establishes a rapport between agents and callers instantaneously

Authentication Through Transfers

Journey utilizes the digital certificates that were created during authentication. They reside with the user, so if the user is transferred between front-office personnel, the identity credentials are stored with the end user and presented, eliminating the need to re-authenticate the user.

- Eliminates a significant pain point for your customers
- Mutually authenticate caller and agent
- Save considerable time by avoiding the repetition of PII
- Compliant with security and privacy requirements

Step Up Authentication

Journey has multiple options to request users to provide additional authentication factors as the transaction risk changes. This is usually invoked when low-risk transactions become high-risk transactions.

As with all Journey solutions, step-up authentication is Zero Knowledge, meaning the inputs are verified but not shown to anyone without the need to know.

- Enable a Zero Knowledge eForm to capture data
- Verify ID documents
- Add in a biometric authentication
- Location Information

Get In Touch

Journey's ground-breaking network and platform approach make almost anything possible. We'd love to talk to you about your challenges with authentication and provide a demo of our capabilities. Visit us at **www.journeyid.com** or **info@journeyid.com**.