Journey

Guide

Journey Authentication Explained

The Journey platform uses the most robust and secure authentication methods available.

The Authentication Foundation

Authenticate the identity of a human being using these factors.

Something you **know**	A shared secret such as a password but is no longer very powerful.
Something you **have**	A mobile device because it is fairly unique to an individual. Use a shared secret and add it to something you have for added security.
Something you **are**	Biometrics including face, voice, and fingerprint.
Some**where** you are	Location, which is in the works.

How does Journey authenticate?

1. **Multifactor**
   - Increases the veracity of the authentication over single factor authentication.
   - Cloud-based authentication reduces the probability of fraud.
2. **Biometrics**
   - Biometrics are hard to steal and cannot be forgotten.
   - Device-based biometrics are a convenience to the user. The device passcode can be used to bypass FaceID (or TouchID). It is better than username and password but not very strong.
   - Cloud-based biometrics cannot be bypassed or reset.
   - As an example, 3D facial maps in combination with a liveness check offer one of the highest veracities of authentication.

Journey Supports

1. **One-time password** sent as an SMS with a 6-digit code that the user has to enter.
2. **Multi-Factor authentication** uses two or more authentication factors.
3. **Mutual authentication** is where the system authenticates both the agent and customer. Each party can then see that the other is authenticated.
4. **Step-up authentication** is a dynamically requested additional authentication.
5. **Continuous authentication** is where authentication happens multiple times during the session. This could be behavioral biometrics, passive voice, or others.

Method	Efficacy
Physiological Biometric ● **Face**: Facial recognition matches different face characteristics of an individual to an approved face. ● **Fingerprint**: a scanner gets an image of your finger, and determines whether the pattern of an the image matches the pattern of in pre-scanned images ● **Voice**: Voice biometrics works by digitizing a profile of a person's speech to produce a stored model voice print, or template.	**Most effective** 3D face map is the most effective Biometric data can’t be cryptographically changed.
Behavioral Biometric ● A variety of sensors in mobile devices to catalog and analyze different behavioral characteristics of an individual, such as gait or typing patterns.	**Very effective**
Knowledge-Based Authentication (KBA) ● **Static** such as SSN number, account number, first pet name but can be socially engineered from public information.	**Effective**

● **Dynamic** is an attempt to make static KBA stronger using **out-of-wallet questions** with access to data from public records.	