

Best Practices to Peacefully (and Successfully) Migrate from Password and Passwordless



Chintan Jain

Senior Director & Head of Cyber Architecture

Hilton

Speaker Introduction

- ❑ Expertise in Consumer Identity, Authentication and related fields
- ❑ Speaker, Mentor & Volunteer
- ❑ Innovator at Heart with 40+ approved patents
- ❑ Granted 9 Patents in Consumer Identity & Authentication
 - a) Government ID card validation systems([US16/150,772](#), [US16/283,157](#), [US16/553,388](#))
 - b) User Authentication by manipulating images of a real scene using augmented reality([US16/000,861](#), [US16/007,284](#), [US16/185,269](#), [US17/338,837](#))
 - c) Systems and methods for providing passwordless login using a random one-time passcode([US15/936,620](#), [US16/237,178](#))

About Hilton



- **150 MILLION HILTON HONORS MEMBERS**
- **GLOBAL FOOTPRINT INCLUDING THE AMERICAS, ASIA PACIFIC (APAC) & EUROPE, MIDDLE EAST & AFRICA (EMEA)**

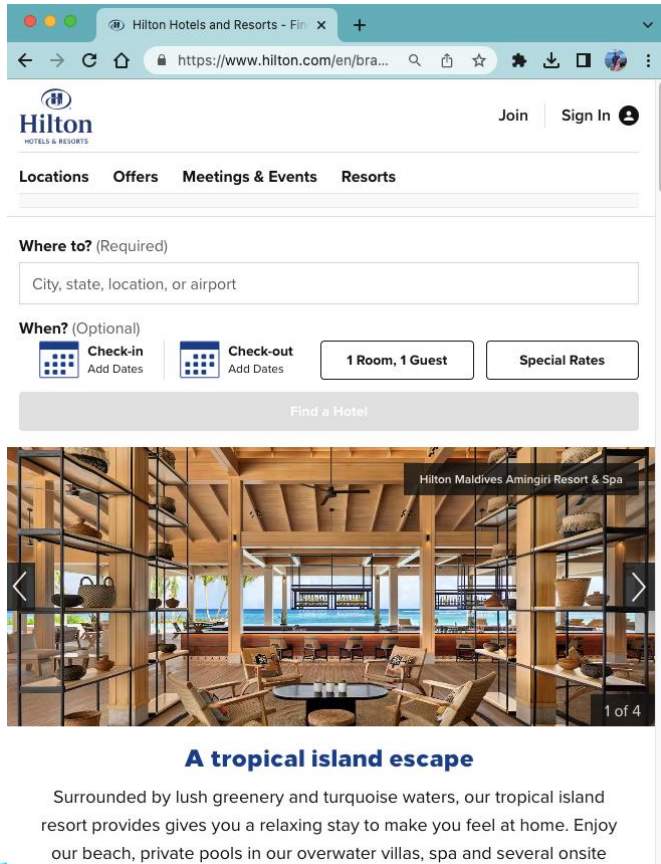
ONE OF THE WORLD'S LARGEST, FASTEST-GROWING HOSPITALITY COMPANIES

19 BRANDS

123 COUNTRIES AND TERRITORIES

7,165 PROPERTIES WORLDWIDE

Hilton customer facing channels



Hilton.com Web Channel

IOS App



Manage your stay



Android App



China IOS App



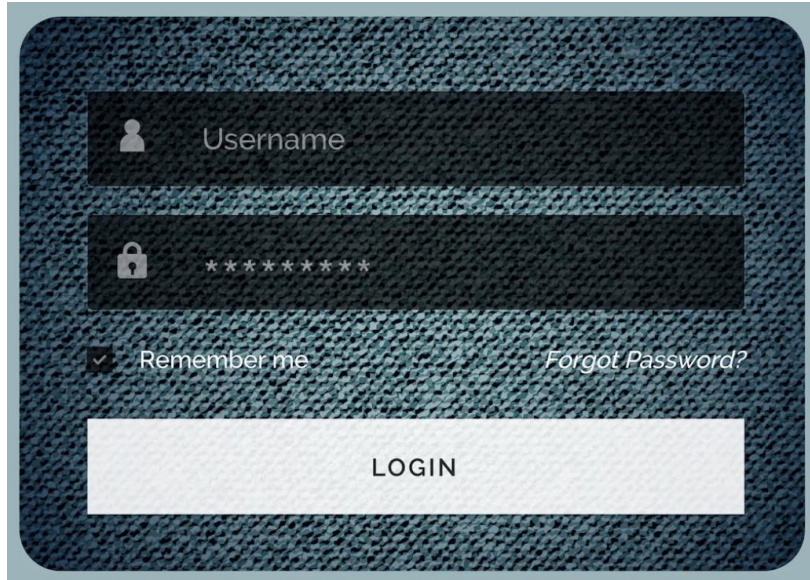
China Android App

WeChat Miniprogram



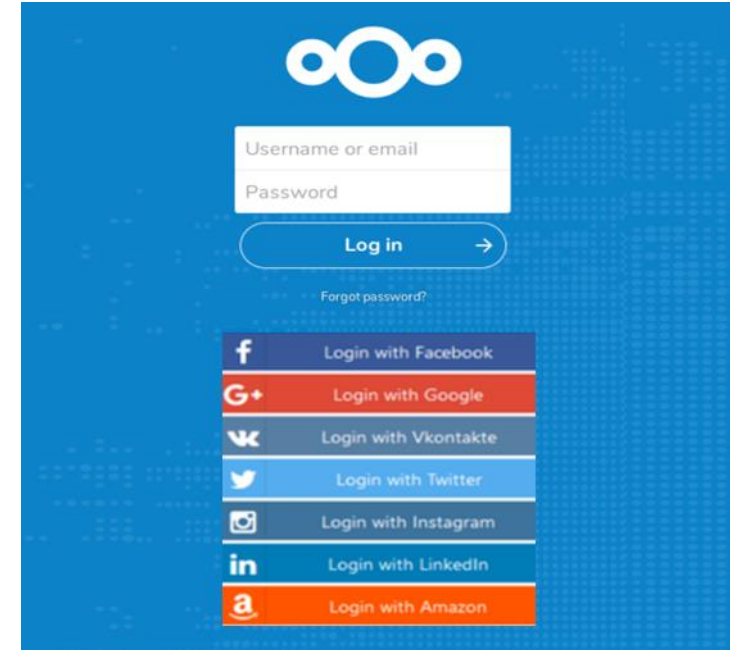
#identiverse

Current ways of consumer authentication

A login form with a dark blue textured background. It features a 'Username' field with a person icon, a password field with a lock icon and masked characters '*****', a 'Remember me' checkbox, a 'Forgot Password?' link, and a large 'LOGIN' button.

Traditional User Name & Password Authentication

- https://www.freepik.com/free-vector/login-form-with-social-networks_1510700.htm#query=login%20with%20facebook&position=1&from_view=search&track=ais

A login form with a blue background and a white logo at the top. It includes fields for 'Username or email' and 'Password', a 'Log in' button with a right arrow, a 'Forgot password?' link, and a vertical stack of social login buttons: 'Login with Facebook', 'Login with Google', 'Login with Vkontakte', 'Login with Twitter', 'Login with Instagram', 'Login with LinkedIn', and 'Login with Amazon'.

Login using Social Login Providers

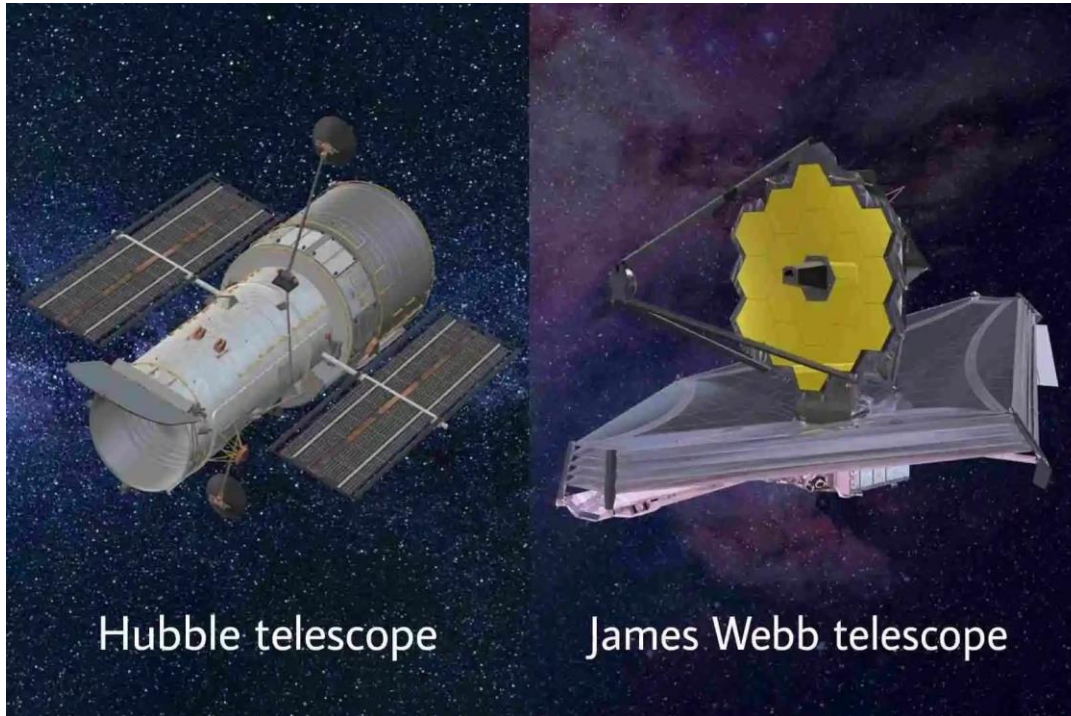
- <https://apps.nextcloud.com/apps/sociallogin> and <http://www.wpfloor.com/wp-content/uploads/2018/08/social-login-2.png>

Current Challenges with Consumer Identity

1. Forgotten Usernames and passwords
2. Billions of Compromised Credentials on Dark Web
3. Account Takeover attacks
4. Phishing & Social engineering of creds
5. Less adoption of Social Login

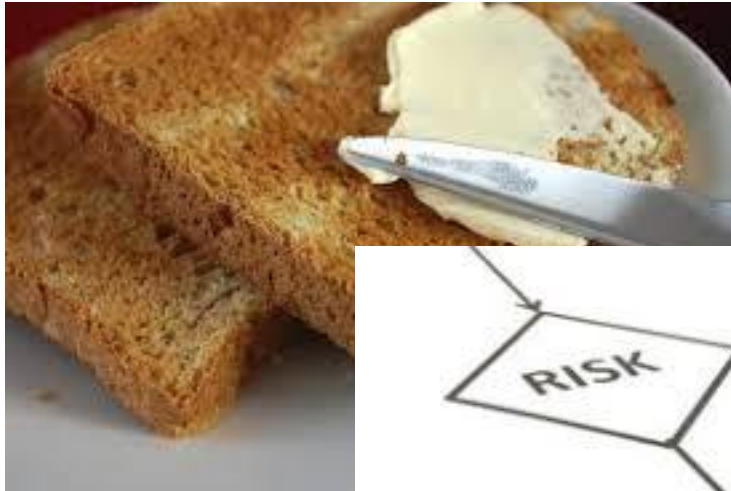
Customers are demanding frictionless ways to login but expect full security and privacy of their accounts

Best practice #1 to rolling out new methods of auth



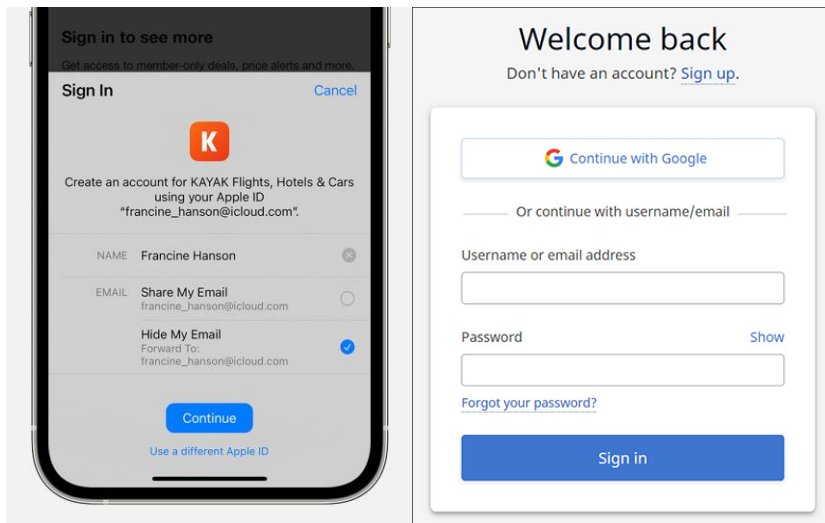
1. Additional Auth methods are complementary
2. Accommodate different devices, OS, Browsers
3. Introduce new flows for new Auth methods
4. Prioritize Consumer Pull over Business Push model

Best practice #2 Add Risk Based Auth



1. User Name/Password is still bread and butter
2. Add risk based authentication when
 - a) Email Address or Phone used as User Name
 - b) A compromised credential
3. Challenge the login transaction with MFA on high risk score

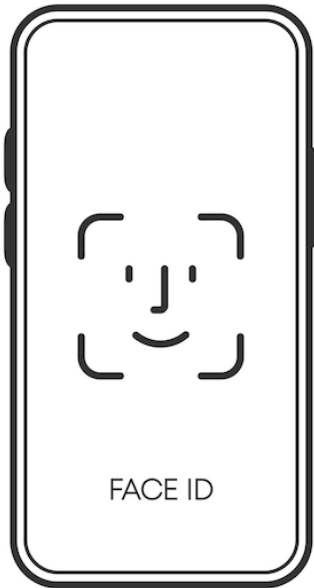
Best practice #3 Offer Social Login from limited providers



1. Offer Social Login from
 - a) Trusted providers
 - b) One or Two providers (e.g. Apple, Google)
2. Localize the social login providers e.g. WeChat in China

<https://support.apple.com/en-us/HT211687>

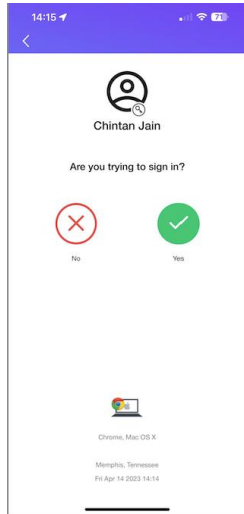
Best practice #4 Enable frictionless login from mobile



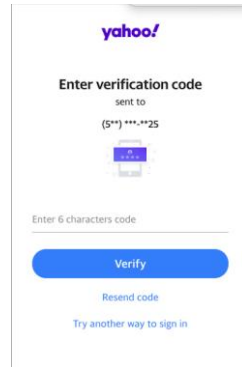
Reduce User Friction from App by

1. Storing User name and password in keychain or secure storage
2. Using Long Lived Refresh Token

Best practice #5 Enable passwordless login using out of band methods

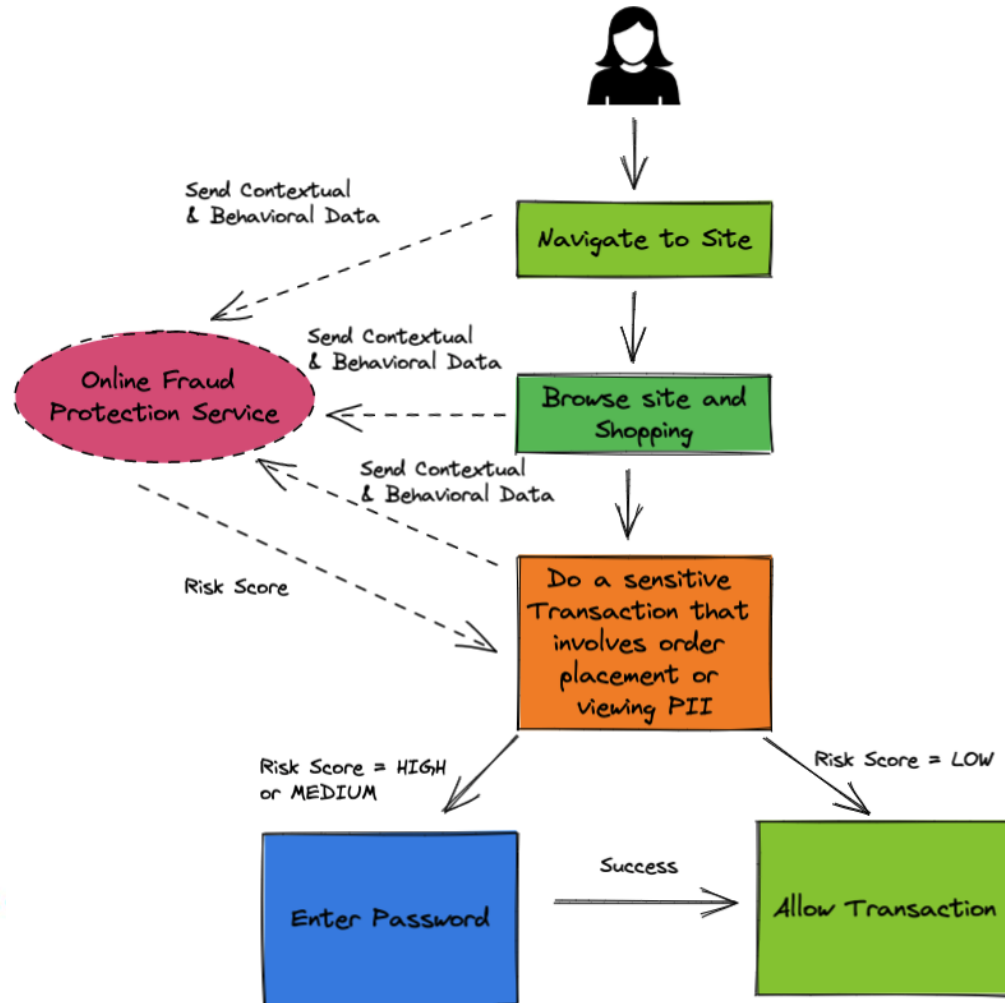


- ☐ Login with Mobile Number/SMS OTP
- ☐ Login with Email/OTP
- ☐ Login with Email/Magic Link



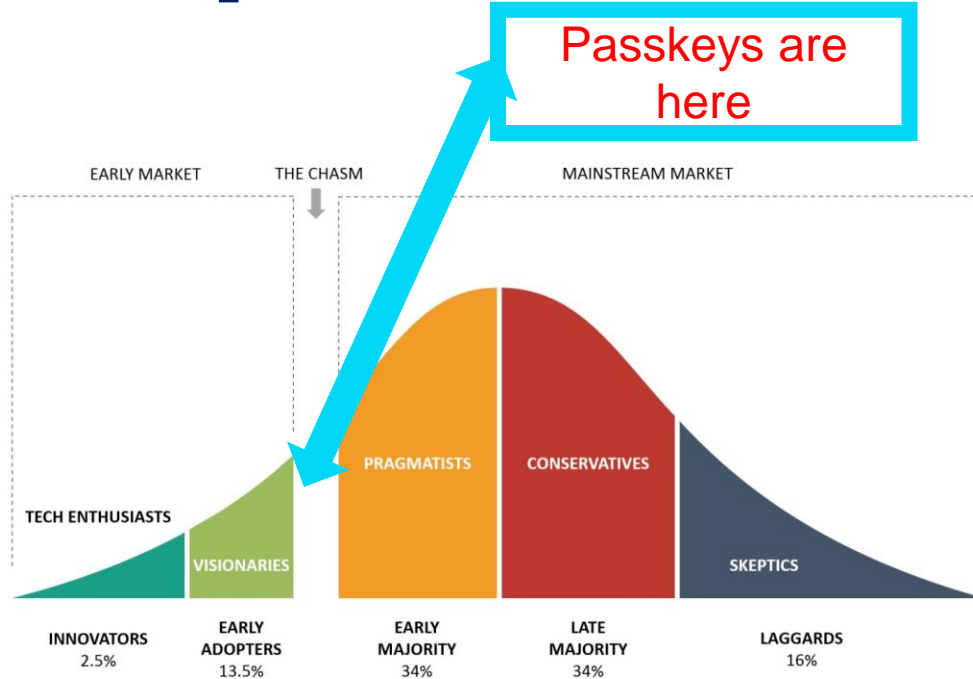
1. Offer Alternate Passwordless methods
2. Account Recovery should be well thought out
3. Enabling this as Auth method takes away Challenge mechanism
 1. Use past business transactions of users to challenge user

Best practice #6 Enable frictionless login from web



1. Reduce sign on prompts
 - a) Use Device, Contextual, Location, data and Passive Behavioral Biometrics
 - b) Use Continuous authentication
2. Challenge user to login if risk score is above threshold

Best practice #7 Start slow Passkey rollout



1. Adopt a wait and watch approach

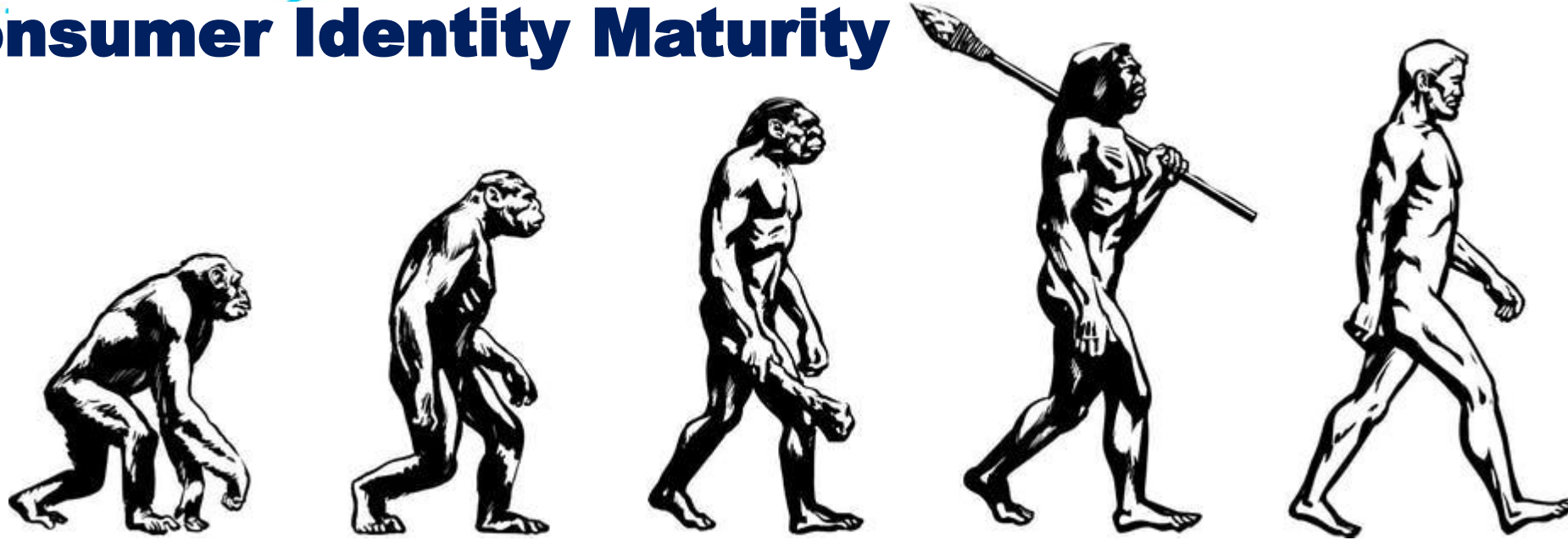
OR

Start slow rollout on iOS and Android App

2. Train your Contact Center staff on Passkeys

1. Global Rollout of Passkeys will be messy
2. Platform and Channel Issues will take time to resolve

Best Practice #8 Continuously Evolve your Consumer Identity Maturity



LEVEL 1

- ☐ AuthN & AuthZ
- ☐ API Access Control
- ☐ Account Registration
- ☐ Password Management
- ☐ Account Management
- ☐ Bot Management

LEVEL 2

- ☐ SSO/SAML
- ☐ OAuth 2.0/Social Login
- ☐ Open ID Connect
- ☐ Adaptive Access
- ☐ ATO Protection
- ☐ Online Fraud Protection
- ☐ Multi Factor Authentication

LEVEL 3

- ☐ Login with Phone/SMS
- ☐ Login with Email
- ☐ Identity Affirmation
- ☐ Identity Proofing

LEVEL 4

- ☐ Journey Time Orchestration
- ☐ Continuous Authentication
- ☐ FIDO & Passkeys
- ☐ Centralized/Decentralized Identity



THANK YOU!