Frontline Team Member Passwordless MFA
ABM at a Glance

Market-leading provider of comprehensive facility services with best-in-class presence and client relationships

- Unparalleled reach
- Diverse commercial portfolio
- Trusted reputation

**Founded in 1909 | $8 billion in revenue**

**350+ US and international locations**

**20,000+ clients | 100,000+ team members**

1. **FACILITIES ENGINEERING**
   - Our 10,000+ certified engineers keep buildings running

2. **JANITORIAL**
   - Each day, we clean 4+ billion sq. ft. of buildings

3. **HVAC & MECHANICAL**
   - We service and maintain 500,000+ heating and cooling systems

4. **MISSION CRITICAL**
   - We service and maintain 35+ million sq. ft. of data center spaces

5. **PARKING & TRANSPORTATION**
   - We collect $2+ billion in parking revenue for our clients

6. **ELECTRICAL**
   - We rank #1 in EV charge port installation in the U.S.

7. **ENERGY**
   - We’ve reduced our client’s average energy use by 30%

8. **LANDSCAPE & TURF**
   - We maintain 55,000+ acres of landscaping & golf courses
We Have a Problem

Problem Statement
• Frontline Team Members (FLTM) are required to log into devices that meet all security requirements for identity and access management.

Functional Requirements
• No email mailboxes
• Shared mobile devices
• Support multiple languages
• Scale, support 100,000+ FLTM

Security Requirements
• Multi-factor Authentication (MFA)
• Single Sign-On (SSO)

Pilot Run
• Conduct the initial pilot in the field with the FLTM
• Captured challenges and lessons learned

• The level of technology knowledge did not support traditional username and password login
Fast, Accurate, & Frictionless Identity-First Security Across All Use Cases

### Passwordless Enterprise
- **Stop MFA Compromise**
  - FIDO2 and Cloud Biometrics stop phishing and MFA push-based attacks

- **Simplify Passwordless Deployments**
  - Self-service enrollment enables fast and secure enterprise-wide deployments

- **Enable Frontline Workers**
  - Seamless MFA for frontline workers on Android and iOS shared devices

### Strong Customer Authentication
- **Stop Account Take Overs**
  - Protect users from phishing and social engineering attacks
  - Secure accounts with Account Owner rooted Biometrics

- **Meet PSD2 and 3DS2 Requirements**
  - Irrefutable audit trail with signed transaction details
  - FIDO2 standard authentication

- **Authenticate Based on Risk**
  - FIDO2 Passkeys
  - Cloud Biometrics
  - Cloud + Passkey

### Frictionless Customer Onboarding
- **Reduced Abandonment**
  - Frictionless liveness and biometric matching
  - 2-sec biometric capture

- **Quickly Identify Customers**
  - 700ms for identity results
  - Largest document support database globally, 13,000+

- **Streamline CIP and KYC**
  - Consolidate compliance under one vendor
Onboarding
Frontline team members (FLTM) go through a simple self-service onboarding process that validates the uniqueness of the biometric and sets machine generated password unknown to any user or system.

Authentication
FLTM scan a QR code located on their badge followed by a biometric capture. Authentication is only allowed from managed ABM-issued devices.

Security + Usability
FLTM perform MFA across shared devices without key fobs, SMS OTP codes or passwords.
Passwordless Authentication is a method that allows frontline team members (FLTM) to gain access to an application or IT system without entering a password or answering security questions. Instead, FLTM provide some other form of evidence such as a fingerprint, proximity badge or hardware token code.

ABM’s Recipe
• Biometrics – Something you are
• QR Code + Device – Something you have

Embedded Benefits
• Multi-factor Authentication
• Single Sign-On
• Elevating the user experience
Lessons Learned

Lesson #1

Business & FLTM-Centric:
The optimal solution resides between business needs, FLTM abilities, and keeping the environment safe from unauthorized access to data, applications and devices.

Lesson #2

Fail Fast: Being agile in identifying and addressing problems quickly gave us time to improve the overall solution to bring value to FLTM.

Lesson #3

Trusted Partnership:
ABM and authID focused on collaboration and thought leadership to work through various challenges.
Thanks to the ABM + authID Team...

- Danyel Anderson, ABM IAM Sr. Director
- Jatinder Batra, ABM Consultant
- Jeremiah Mason, authID Chief Product Officer
- Kristina Coyle, ABM IAM Sr. Architect
- Marie Paterson, ABM Enterprise Change Consultant
- Max Umarov, authID SVP Solutions Engineering
- Michael Harewood, ABM System Engineer
- Paul Quach, ABM IAM Engineer
- Randy Reams, ABM Client Computing Engineer
- Stephanie Franklin-Thomas, ABM SVP & CISO
- Taylor Alsobrook, ABM Sr. System Engineer
- Thomas Szoke, authID Chief Technology Officer & Founder