Multi-Factor Authentication (MFA) Implementation

Hatch Labs Holdings LLC

Product: AmandasList — Verified Membership Network

Document Version: 1.0 | Effective Date: March 6, 2026

Classification: Confidential

1. Overview

Hatch Labs Holdings LLC ("Company") implements multi-factor authentication (MFA) across all critical systems that store, process, or transmit consumer data. MFA is required for both internal administrative access and consumer-facing applications before any financial data is accessed via Plaid Link.

2. Consumer-Facing MFA

All AmandasList users must complete multi-factor authentication before accessing Plaid Link or any financial verification features.

2.1 Authentication Flow

Step	Method	Description
1. Primary Authentication	Email + Password	User logs in with registered email and password (minimum 8 characters, complexity requirements enforced)
2. Second Factor	SMS OTP / Email OTP	6-digit one-time passcode sent via SMS or email. Valid for 10 minutes. Rate-limited to 5 attempts per hour.
3. Plaid Link Access	Session Verified	Plaid Link is only surfaced after successful MFA completion. Session tokens expire after 30 minutes of inactivity.

2.2 MFA Enforcement Policy

- MFA is **mandatory** for all users — cannot be disabled
- MFA is required on every new device or browser
- MFA is re-prompted before any financial data access or Plaid Link interaction

- Failed MFA attempts are logged and trigger account lockout after 5 consecutive failures

2.3 Implementation Technology

Consumer MFA is implemented using **Supabase Auth**, which provides:

- Built-in MFA support (TOTP and SMS-based OTP)
- Session management with configurable timeouts
- Rate limiting and brute-force protection
- Audit logging of all authentication events

3. Internal Systems MFA

All internal systems that store or process consumer financial data require MFA for administrative access.

System	Purpose	MFA Method	Status
Supabase Dashboard	Database administration, consumer data management	Email OTP / Authenticator App	✓ **Active**
Google Workspace	Business email, document management	Google 2-Step Verification (SMS + Authenticator)	✓ **Active**
Mercury Bank	Business banking, financial operations	Authenticator App + Backup Codes	✓ **Active**
GitHub	Source code, deployment pipeline	Authenticator App / SMS	✓ **Active**
Cloudflare	DNS, CDN, SSL/TLS management	Email OTP / Authenticator App	✓ **Active**
Plaid Dashboard	API key management, integration monitoring	Email OTP / Authenticator App	✓ **Active**

4. MFA Policy Requirements

4.1 Acceptable Second Factors

- **Time-based One-Time Passwords (TOTP)** — via authenticator apps (Google Authenticator, Authy, 1Password)
- **SMS-based OTP** — 6-digit codes delivered via SMS
- **Email-based OTP** — 6-digit codes delivered via registered email

4.2 Session Management

- Authenticated sessions expire after 30 minutes of inactivity
- Maximum session duration: 24 hours (re-authentication required)
- Session tokens are cryptographically signed and stored securely
- Sessions are invalidated on password change or account modification

4.3 Account Recovery

- Lost MFA devices: recovery via verified email with identity confirmation
- Backup codes: generated at MFA enrollment (one-time use, stored securely)
- Admin recovery: manual identity verification required before MFA reset

5. Monitoring and Logging

- All MFA events (success, failure, enrollment, recovery) are logged with timestamp, IP address, and device fingerprint
- Failed MFA attempts generate alerts after 3 consecutive failures
- Account lockout after 5 consecutive MFA failures (30-minute cooldown)
- Logs retained for minimum 12 months for audit and compliance purposes

6. Compliance

This MFA implementation aligns with:

- **NIST SP 800-63B** — Digital Identity Guidelines (Authentication and Lifecycle Management)
- **SOC 2 Type II** — via Supabase's certified infrastructure
- **CCPA** — California Consumer Privacy Act security requirements
- **Plaid Security Requirements** — as specified in the Plaid Partner Security Questionnaire

7. Review Schedule

This MFA implementation is reviewed:

- **Quarterly:** Access logs reviewed for anomalies
- **Annually:** Full policy review and update
- **As needed:** After any security incident or significant infrastructure change

---

This document is confidential and intended for authorized recipients only.