Data Retention and Disposal Policy

Hatch Labs Holdings LLC

Product: AmandasList — Verified Membership Network

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

Next Review Date: March 6, 2027

Classification: Confidential

1. Purpose

This policy establishes the requirements for retention, deletion, and disposal of data collected, processed, and stored by Hatch Labs Holdings LLC ("Company") in connection with the AmandasList platform. This policy ensures compliance with applicable data privacy laws, including the California Consumer Privacy Act (CCPA), and contractual obligations with third-party service providers including Plaid, Inc.

2. Scope

This policy applies to all data collected and processed by AmandasList, including:

- Consumer personal information (name, email, phone number, date of birth)
- Financial data retrieved via Plaid API (identity verification, income, asset, and account data)
- Authentication and session data
- Usage data and application logs
- Internal business records

3. Data Classification and Retention Schedule

Data Category	Examples	Retention Period	Disposal Method
Consumer Identity Data	Name, email, phone, DOB, address	Duration of active account + 30 days after deletion request	Permanent deletion from database and all backups within 30 days

Plaid Financial Data	Account balances, income verification, identity verification results	Duration of active account; deleted within 30 days of account closure or deletion request	Permanent deletion from database; Plaid access tokens revoked immediately
Plaid Access Tokens	API tokens linking to consumer financial institutions	Duration of active account; revoked immediately upon account deletion	Token revocation via Plaid API; removal from database
Authentication Data	Hashed passwords, MFA enrollment, session tokens	Duration of active account; deleted with account	Permanent deletion; session tokens invalidated immediately
Verification Results	Pass/fail verification status, verification timestamps	Duration of active account + 90 days (for dispute resolution)	Permanent deletion from database
Application Logs	API access logs, authentication events, error logs	12 months from creation	Automated purge from logging infrastructure
Usage Analytics	Feature usage, session duration, anonymized behavioral data	24 months (anonymized/aggregated data may be retained indefinitely)	Deletion of raw data; aggregated statistics retained
Support Communications	Customer support tickets, email correspondence	Duration of active account + 12 months	Permanent deletion from support systems
Legal/Compliance Records	Consent records, terms acceptance, regulatory filings	7 years from date of creation (per IRS and state requirements)	Secure destruction after retention period
Business Financial Records	Invoices, payment records, tax documents	7 years (per IRS requirements)	Secure destruction after retention period

4. Consumer Data Deletion Rights

4.1 Right to Delete

Consumers may request deletion of their personal data at any time by:

- Using the in-app account deletion feature
- Emailing amanda@hatchlabs.com with subject line "Data Deletion Request"

4.2 Deletion Process

Step	Action	Timeline
1	Receive and verify deletion request (confirm identity of requester)	Within 48 hours
2	Revoke Plaid access tokens and disconnect financial institution links	Immediately upon verification
3	Delete consumer personal data from primary database	Within 7 business days
4	Delete consumer data from backups	Within 30 calendar days
5	Send deletion confirmation to consumer	Upon completion of step 3

4.3 Exceptions to Deletion

The Company may retain limited data after a deletion request to:

- Complete a transaction or provide a requested service
- Comply with legal obligations (e.g., tax records, fraud prevention)
- Detect and resolve security incidents
- Exercise or defend legal claims

Any retained data will be limited to the minimum necessary and will be deleted once the legal basis for retention expires.

5. Data Disposal Methods

5.1 Electronic Data

- **Database records:** Permanent deletion using SQL DELETE operations followed by verification that records are no longer retrievable
- **Encrypted data:** Cryptographic erasure (destruction of encryption keys) where applicable
- **Backups:** Data removed from backup sets during next backup rotation cycle (maximum 30 days)
- **Logs:** Automated log rotation and purge per retention schedule

5.2 Third-Party Data

- **Plaid:** Access tokens revoked via API; Plaid's own retention policies apply to data held by Plaid (see Plaid End User Privacy Policy)
- **Supabase:** Data deleted from Supabase-hosted database; Supabase's infrastructure-level backups follow their data retention policies

6. Plaid-Specific Data Handling

In accordance with Plaid's data access requirements:

- Financial data retrieved from Plaid is used **solely** for identity and income verification purposes
- Raw financial data (account numbers, routing numbers) is **never stored** — only verification results (pass/fail) are retained
- Plaid access tokens are stored encrypted at rest (AES-256) and are revoked immediately upon account deletion
- The Company does not share Plaid-retrieved data with any third parties
- The Company does not use Plaid data for marketing, advertising, or any purpose beyond verification

7. Policy Enforcement

- The CEO/Chief Security Officer is responsible for enforcement of this policy
- Automated retention rules are implemented in the database where technically feasible
- Manual reviews are conducted quarterly to ensure compliance
- Violations of this policy may result in disciplinary action up to and including termination

8. Policy Review

- **Annual review:** This policy is reviewed and updated at minimum once per year
- **Trigger-based review:** Policy is also reviewed upon any material change to data processing activities, applicable laws, or third-party service provider agreements
- **Next scheduled review:** March 6, 2027

9. Applicable Laws and Regulations

- California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA)
- Gramm-Leach-Bliley Act (GLBA) — to the extent applicable to financial data handling

- IRS record retention requirements (26 CFR § 1.6001-1)
- Texas Business and Commerce Code — data breach notification
- Plaid contractual data handling requirements

Hatch Labs Holdings LLC | 701 Tillery Street, Suite 12, Austin TX 78702 | amanda@hatchlabs.com

Document Owner: Amanda Bradford, CEO & Chief Security Officer

Approved: Amanda Bradford | Date: March 6, 2026