Data Deletion & Retention Policy

Effective date: February 2026 **Owner:** Crumbs Money Engineering **Review cadence:** Annually or after any material change to data practices **Applicable law:** California Consumer Privacy Act (CCPA/CPRA), state-level privacy laws (Virginia VCDPA, Colorado CPA, Connecticut CTDPA, etc.), Gramm-Leach-Bliley Act (GLBA) safeguards

---

1. Purpose

This policy defines what personal and financial data Crumbs Money collects, how long it is retained, when and how it is deleted, and how users can exercise their data rights under applicable U.S. privacy laws. Crumbs Money is a read-only personal finance dashboard — we never initiate transfers, move funds, or store bank login credentials.

---

2. Scope

This policy applies to all data collected, processed, or stored by Crumbs Money, including:

- User identity data (Firebase UID, Google profile information)
- Financial account data (Plaid access tokens, account metadata)
- Transaction data (synced from Plaid)
- Application logs and operational data

---

3. Categories of data collected

Category	Data elements	Source	Purpose
Identity	Firebase UID, display name, email (via Google SSO)	Firebase Authentication	Authenticate users, scope data access
Financial connection	Plaid `access_token`, `item_id`, `institution_name`, `sync_cursor`, `last_synced_at`	Plaid API	Maintain connection to user's financial institution
Transaction history	Transaction name, amount, date, account ID, account name	Plaid Transactions Sync	Display spending history to the user
Live financial data	Account balances, investment holdings	Plaid API (fetched on demand)	Display current balances and holdings — **not stored**
Operational	Server logs, error messages	Application runtime	Debugging and monitoring — **no sensitive data logged**

Data we never collect or store:

- Bank login credentials (handled entirely by Plaid Link)
- Social Security numbers
- Full account or routing numbers
- User passwords (authentication delegated to Google)

---

4. Retention schedule

Data type	Retention period	Trigger for deletion
Plaid access tokens	Active connection lifetime	User disconnects the connection
Transaction history	Active connection lifetime	User disconnects the connection
Plaid sync cursor	Active connection lifetime	User disconnects the connection
Firebase UID (in our DB)	Until all connections are removed	Last connection disconnected removes all user rows
Account balances & holdings	Not retained	Fetched live per request, never written to database
Application logs	Rolling 30-day window	Automatic expiration via hosting platform (Railway)

Principle: We retain user financial data only for as long as the user maintains an active connection. We do not retain financial data for analytics, model training, or any secondary purpose.

---

5. User-initiated deletion

5.1 Disconnect a financial connection

Users can disconnect any linked financial institution at any time through the application interface.

What happens when a user disconnects:

1. All transaction records associated with that connection are permanently deleted from the database (`DELETE FROM transactions WHERE item_id = $1`).
2. The Plaid item record (including the access token and sync cursor) is permanently deleted from the database (`DELETE FROM plaid_items WHERE item_id = $1`).
3. The Plaid access token is revoked via Plaid's `/item/remove` API, instructing Plaid to invalidate the token and stop data access.
4. No financial data for that connection is retained after disconnection.

5.2 Full account deletion request

Users may request complete deletion of all their data by contacting us. Upon receiving a verified deletion request:

1. All connected Plaid items are disconnected (access tokens revoked via Plaid `/item/remove`).
2. All transaction records for the user are permanently deleted.
3. All Plaid item records for the user are permanently deleted.
4. Firebase Authentication record can be deleted through Firebase Admin SDK upon request.
5. Deletion is completed within **30 calendar days** of the verified request, consistent with CCPA requirements.

5.3 Verification of deletion requests

To prevent unauthorized deletion, we verify the identity of the requester by:

- Confirming the request originates from the authenticated user's Google account, or
- Matching the request email to the Firebase UID on record.

---

6. Automated deletion

Scenario	Action
User disconnects a connection	Immediate deletion of all associated data (see 5.1)
Plaid access token becomes permanently invalid	Item and associated transactions are flagged for cleanup
Application logs older than 30 days	Automatically purged by Railway's log retention policy

---

7. Third-party data sharing & sub-processors

Crumbs Money does **not** sell, rent, or share user personal or financial data with third parties for marketing, advertising, or any secondary commercial purpose.

Third party	Data shared	Purpose	Their retention
Plaid	User's bank credentials are entered directly in Plaid Link (never touch our servers). We hold an opaque `access_token`.	Financial data aggregation	Governed by Plaid's Privacy Policy. Users can revoke access via Plaid Portal or by disconnecting in our app.
Firebase (Google)	User identity (Google account info)	Authentication	Governed by Google's Privacy Policy. Users can revoke app access in Google Account settings.
Railway	Application code, environment variables, database storage	Hosting & infrastructure	Governed by Railway's Privacy Policy. Data deleted when resources are removed.

---

8. CCPA/CPRA consumer rights

Crumbs Money supports the following consumer rights under the California Consumer Privacy Act as amended by the California Privacy Rights Act:

Right	How we fulfill it
Right to know	Users can view all their stored data (connections, transactions) directly in the application dashboard.
Right to delete	Users can disconnect individual connections (immediate deletion) or request full account deletion (completed within 30 days). See Section 5.

Right to correct	Financial data is sourced from Plaid and reflects the source institution. Users should correct data at their bank. We do not manually modify synced financial data.
Right to opt out of sale/sharing	We do not sell or share personal information for cross-context behavioral advertising. No opt-out mechanism is needed because no sale or sharing occurs.
Right to limit use of sensitive personal information	Financial data is used solely to display it back to the authenticated user. No secondary use occurs.
Non-discrimination	We do not discriminate against users who exercise their privacy rights.

---

9. State privacy law compliance

In addition to CCPA/CPRA, Crumbs Money complies with the following state privacy laws to the extent applicable:

Law	Jurisdiction	Key requirements met
VCDPA	Virginia	Right to access, delete, correct, opt out. Data protection assessment not triggered (we do not sell data or process for targeted advertising).
CPA	Colorado	Right to access, delete, correct, opt out. Universal opt-out mechanism not needed (no sale/sharing).
CTDPA	Connecticut	Right to access, delete, correct, opt out.
UCPA	Utah	Right to access, delete, opt out of sale.
GLBA (Safeguards Rule)	Federal	Financial data protected by access controls, encryption at rest and in transit, incident response procedures. See Information Security Policy.

---

10. Data breach notification

In the event of a data breach involving personal or financial information:

1. **Assessment** — Determine scope, affected users, and data types exposed within 72 hours.
2. **Notification to users** — Notify affected California residents within the timeframe required by the California Civil Code § 1798.82 (without unreasonable delay). Notify residents of other states per their respective breach notification statutes.
3. **Notification to regulators** — If the breach affects 500+ California residents, notify the California Attorney General. Comply with other state AG notification requirements as applicable.
4. **Notification to Plaid** — If Plaid access tokens are potentially compromised, notify Plaid's security team (security@plaid.com) and revoke affected tokens.
5. **Documentation** — Record the incident, root cause, remediation, and preventive measures per the Information Security Policy.

---

11. Data processing safeguards

To ensure data is handled securely throughout its lifecycle:

- **Encryption at rest:** All database storage (PostgreSQL on Railway) uses AES-256 encryption.
- **Encryption in transit:** All network communication uses HTTPS/TLS.
- **Access controls:** All API endpoints require authenticated Firebase ID tokens. All database queries are scoped by verified user ID.
- **Minimization:** We collect only the data necessary to provide the service. We do not store balances or holdings — they are fetched live and never persisted.
- **Parameterized queries:** All database operations use parameterized SQL to prevent injection.
- **No secondary use:** Financial data is used exclusively to display it to the authenticated user. We do not use it for analytics, profiling, advertising, or model training.

---

12. Policy updates

- This policy is reviewed annually and updated after any material change to data collection, storage, or sharing practices.
- Material changes are communicated to users through the application.
- Prior versions of this policy are archived for reference.

---

13. Contact

For data deletion requests, privacy inquiries, or to exercise any rights described in this policy, contact:

Crumbs Money Privacy Email: david.lietjauw@gmail.com

Last updated: February 2026