Data Storage & Security Overview

Where Information is Stored

1. Customer Device (Mobile App)

What's Stored:

- Biometric templates (face/voice patterns)
- Device fingerprint
- Encrypted authentication tokens
- Shopping preferences

Security:

- Secure hardware enclave
- Data never leaves device
- Automatic deletion after 90 days of inactivity

2. Bank's Secure Servers

What's Stored:

- Customer account information
- Spending limits and delegation rules
- Transaction history
- Fraud detection patterns
- Compliance audit logs

Security:

- Bank-grade encryption (AES-256)
- Hardware Security Modules (HSM)
- Regular security audits
- Compliance with banking regulations

3. CallSign Authentication Service

What's Stored:

- Behavioral authentication patterns
- Device risk scores
- Authentication session logs

Security:

- Encrypted behavioral patterns only
- No personal identifiable information
- Data retention: 12 months maximum

4. Retailer Systems (Amazon, BestBuy, Target)

What's Stored:

- Product search queries
- Purchase confirmations
- Delivery information

Security:

- Standard e-commerce encryption
- Bank-verified payment tokens only
- No direct access to bank account details

Data Protection Principles

- **Minimal Data Collection:** Only essential information is stored
- **Purpose Limitation:** Data used only for intended banking/shopping services
- **Retention Limits:** Automatic deletion based on regulatory requirements
- **Customer Control:** Users can revoke permissions and delete data anytime
- **Regulatory Compliance:** Meets all banking privacy and security standards

Customer Rights

- View all stored data
- Delete account and all associated data
- Revoke AI agent permissions
- Export transaction history
- Report security concerns directly to bank