MG9 GROUP LLC

DATA RETENTION AND DISPOSAL POLICY

Effective Date: April 22, 2026

Version: 1.0

Document Classification: CONFIDENTIAL

DOCUMENT CONTROL

Field	Details
Version	1.0
Effective Date	April 22, 2026
Author	Data Protection Officer / Compliance Team
Approver	Chief Executive Officer
Status	Approved
Review Cycle	Annual (next review: April 2027)
Distribution	All employees, contractors, and authorized third parties

Version History

Version	Date	Author	Description of Changes
1.0	April 22, 2026	Data Protection Officer	Initial policy creation and approval

1.0 PURPOSE AND SCOPE

1.1 Purpose

This Data Retention and Disposal Policy ("**Policy**") establishes the guidelines, standards, and procedures governing the retention, storage, and secure disposal of all data collected, processed, or stored by MG9 Group LLC ("**MG9**" or the "**Company**") in connection with its business operations and its integration with Plaid Inc.'s ("**Plaid**") financial data services and application programming interfaces ("**APIs**").

The purpose of this Policy is to ensure that MG9 Group LLC:

- Retains data only for as long as necessary to fulfill defined business, legal, and regulatory obligations;
- Protects the confidentiality, integrity, and availability of all data throughout its lifecycle;
- Disposes of data securely and irreversibly when retention periods expire;
- Complies with all applicable federal, state, and industry-specific regulations; and
- Maintains compliance with Plaid's Developer Policy and security requirements for authorized integrators.

1.2 Scope

This Policy applies to:

- All employees, officers, and directors of MG9 Group LLC;
- All contractors, consultants, and temporary workers engaged by MG9 Group LLC;
- All third-party service providers, vendors, and subprocessors who handle MG9 Group LLC data;
- All information systems, databases, applications, cloud environments, and physical storage media that contain Company or customer data; and
- All data formats, including electronic records, paper documents, backups, archives, and any copies or derivatives thereof.

1.3 Regulatory Alignment

This Policy has been developed in alignment with the following laws, regulations, standards, and industry frameworks:

- **Plaid Developer Policy** — Requirements for authorized developers and integrators accessing Plaid APIs;
- **SOC 2 Trust Services Criteria** — Criteria for security, availability, processing integrity, confidentiality, and privacy;
- **ISO 27001:2022** — Information security management systems requirements;
- **ISO 27701:2019** — Privacy information management extension to ISO 27001;
- **Gramm-Leach-Bliley Act (GLBA)** — Financial data privacy and safeguarding requirements;

- **California Consumer Privacy Act / California Privacy Rights Act (CCPA/CPRA)** — Consumer data rights and protection;
- **Consumer Financial Protection Bureau (CFPB) Regulations** — Consumer financial data protections;
- **NIST Special Publication 800-88 Rev. 1** — Guidelines for media sanitization;
- **Bank Secrecy Act / Anti-Money Laundering (BSA/AML)** — Financial record-keeping obligations;
- **Internal Revenue Code (IRC) §6501** — Tax record retention requirements; and
- **Sarbanes-Oxley Act (SOX)** — Financial record retention and integrity.

2.0 DEFINITIONS

The following terms, as used throughout this Policy, shall have the meanings set forth below:

"Personal Data" means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to an identified or identifiable natural person or household, as defined under CCPA/CPRA and other applicable privacy laws.

"End User Data" means any data pertaining to an end user that is retrieved, transmitted, or otherwise obtained through Plaid's APIs and services, including but not limited to financial account information, transaction data, identity data, and authentication credentials, as defined in and governed by Plaid's Developer Policy.

"Financial Data" means any data relating to the financial accounts, transactions, balances, assets, liabilities, income, or other financial

attributes of an individual or entity, whether obtained through Plaid or through other means.

"Plaid Access Tokens" means the persistent API tokens issued by Plaid upon successful user authentication via Plaid Link, which authorize ongoing access to a specific end user's connected financial accounts.

"Sensitive Data" means any subset of Personal Data that presents a heightened risk of harm if disclosed, including Social Security numbers, financial account numbers, government-issued identification numbers, biometric data, and authentication credentials.

"Data Controller" means the entity that determines the purposes and means of processing Personal Data. For the purposes of this Policy, MG9 Group LLC acts as the Data Controller with respect to End User Data collected through Plaid integrations.

"Data Processor" means the entity that processes Personal Data on behalf of the Data Controller. Third-party vendors and subprocessors engaged by MG9 Group LLC act as Data Processors.

"Data Subject" means the identified or identifiable natural person to whom Personal Data relates, including end users of MG9 Group LLC's applications and services.

"Retention Period" means the defined duration for which a specific category of data is authorized to be stored by MG9 Group LLC, as specified in Section 4.0 of this Policy.

"Disposal" means the permanent and irreversible removal or destruction of data from all storage media, such that the data cannot be recovered, reconstructed, or accessed by any means.

"Sanitization" means the process of removing data from storage media using methods that render the data unrecoverable, in accordance with NIST SP 800-88 Rev. 1 guidelines, including Clear, Purge, and Destroy methods.

"Cryptographic Erasure" means the process of rendering encrypted data permanently inaccessible by securely destroying all copies of the encryption

key(s) used to protect the data, thereby rendering the ciphertext unrecoverable.

2.1 Data Classification Levels

MG9 Group LLC classifies all data into one of four levels, which govern handling, storage, access, and disposal requirements:

- **"Public"** — Data intended for unrestricted public dissemination, the unauthorized disclosure of which would have no adverse impact on the Company.
- **"Internal"** — Data intended for use within MG9 Group LLC that is not intended for public release, the unauthorized disclosure of which could cause minor adverse impact.
- **"Confidential"** — Data that is sensitive in nature, the unauthorized disclosure of which could cause significant adverse impact to MG9 Group LLC, its customers, or its partners.
- **"Restricted"** — Data that is highly sensitive, the unauthorized disclosure of which could cause severe adverse impact, including regulatory penalties, financial loss, or significant reputational harm. This is the highest classification level.

3.0 DATA CLASSIFICATION FRAMEWORK

3.1 Classification Levels and Examples

All data handled by MG9 Group LLC shall be classified according to the following framework. Classification determines the applicable security controls, access restrictions, retention periods, and disposal methods.

Classification Level	Description	Examples (Fintech Context)	Handling Requirements
Restricted	Highest sensitivity. Unauthorized disclosure would cause severe harm including regulatory penalties and significant financial loss.	Plaid access tokens; bank account numbers and routing numbers; Social Security numbers; authentication credentials; encryption keys; KMS master keys	Encrypted at rest (AES-256) and in transit (TLS 1.2+); column-level encryption for tokens; MFA required; access logged and audited; two-person integrity for disposal; need-to-know access only
Confidential	High sensitivity. Unauthorized disclosure could cause significant adverse impact to the Company or its customers.	Transaction histories; account balances; identity verification data (name, DOB, address from Plaid Identity); consent records; financial reports; customer PII; API logs containing user data	Encrypted at rest and in transit; role-based access control; access requires business justification; quarterly access reviews; secure disposal required
Internal	Moderate sensitivity. Intended for internal use only. Unauthorized disclosure could cause minor adverse impact.	Internal reports and memoranda; employee records; internal system documentation; non-production environment configurations; vendor contracts; meeting minutes; internal communications	Restricted to authorized personnel; standard access controls; encrypted in transit; secure disposal when no longer needed

Classification Level	Description	Examples (Fintech Context)	Handling Requirements
Public	No sensitivity. Intended for unrestricted dissemination. No adverse impact from disclosure.	Published marketing materials; public website content; press releases; public API documentation; job postings	No special handling required; standard business practices apply; verify accuracy before publication

3.2 Classification Assignment

Data classification shall be assigned at the point of creation or collection. The data owner is responsible for ensuring accurate classification. When data of multiple classification levels is combined, the combined dataset shall be classified at the highest level present. Classification decisions shall be reviewed during quarterly access reviews and updated as necessary to reflect changes in data sensitivity or regulatory requirements.

4.0 DATA CATEGORIES AND RETENTION SCHEDULE

The following table specifies the authorized retention periods for each category of data processed by MG9 Group LLC. All retention periods are measured from the specified trigger event. Upon expiration of the retention period, data shall be disposed of in accordance with Section 7.0 of this Policy unless a legal hold is in effect.

Data Category	Description & Examples	Classification	Retention Period	Legal / Business Justification	Disposal Method
Plaid Access Tokens & API Credentials	Persistent tokens issued by Plaid for ongoing account access; API keys, client secrets, and webhook verification tokens	Restricted	Active connection duration only. Revoked and deleted immediately upon user disconnection, account deactivation, or revocation of consent.	Plaid Developer Policy; principle of least privilege; minimization of exposure window for financial account access	Programmatic revocation via Plaid API (`/item/remove`); cryptographic erasure from all storage; deletion verified across all replicas
End User Financial Data	Transactions, balances, account information, and investment data retrieved via Plaid APIs	Confidential	3 years from date of collection or date of last user activity, whichever is later	GLBA record-keeping requirements; CFPB complaint retention (3 years); business analytics and customer service continuity	Cryptographic erasure; secure database deletion with verification; removal from backups within 90 days
Identity Verification Data	Full name, date of birth, Social Security number, address, and other identity attributes	Restricted	5 years from account closure or date of last verification event, whichever is later	BSA/AML (31 CFR §1010.430 — 5-year retention); KYC/CDD requirements; CFPB regulatory compliance	Cryptographic erasure; NIST 800-88 Purge-level sanitization; two-person verificatio

Data Category	Description & Examples	Classification	Retention Period	Legal / Business Justification	Disposal Method
	obtained via Plaid Identity or direct collection for KYC purposes			e	n of disposal
Transaction & Payment Records	Records of payments processed, invoices, receipts, billing statements, and associated financial transaction documentation	Confidential	7 years from transaction date	IRS record-keeping (IRC §6501 — 3-year statute, 6-year extended); SOX Section 802 (7 years); state tax authority requirements	Cryptographic erasure; secure deletion with audit trail
User Account Data	Email addresses, phone numbers, login credentials (hashed), user preferences, account settings, and profile information	Confidential	Duration of active account plus 1 year following account closure or deactivation	Customer support continuity; dispute resolution window; CCPA/CPRA compliance for post-closure requests	Secure database deletion; cryptographic erasure; removal from backups within 90 days

Data Category	Description & Examples	Classification	Retention Period	Legal / Business Justification	Disposal Method
Audit Logs & Security Logs	System access logs, authentication logs, change management logs, security event logs, and administrative action records	Confidential	3 years minimum from date of log entry	SOC 2 Trust Services Criteria (CC7.2 — monitoring); ISO 27001 Annex A.12.4 (logging and monitoring); security incident investigation requirements	Secure deletion; cryptographic erasure from log management systems and archives
Consent Records	Records of Plaid Link consent events, privacy notice acknowledgments, terms of service acceptance, data sharing authorizations, and opt-in/opt-out records	Confidential	7 years from date of consent event	GLBA (12 CFR §1016); CCPA/CPRA (Cal. Civ. Code §1798.185); Plaid Developer Policy evidence of user authorization	Secure deletion with audit trail; archive before disposal
API Request/ Response Logs	Logs of API calls to/from Plaid and	Internal	1 year from date of request	Application debugging and	Automated deletion via log rotation;

Data Category	Description & Examples	Classification	Retention Period	Legal / Business Justification	Disposal Method
	internal services, including request metadata, response codes, and performance metrics (excluding raw financial data)			troubleshooting; security monitoring and anomaly detection; SOC 2 monitoring controls	secure deletion from log aggregation platforms
Employee & Contractor Records	Employment agreements, performance reviews, tax forms (W-2, W-4, 1099), benefits records, background checks, and training records	Internal	Duration of employment or engagement plus 7 years following separation	IRS record-keeping (IRC §6001); Department of Labor (29 CFR §516.5); state employment law; EEOC (Title VII — 1 year minimum)	Cross-cut shredding for paper (DIN 66399 P-4); secure deletion for electronic records
Business Communications	Corporate emails, instant messages, internal memoranda, and official correspondence related to business	Internal	3 years from date of communication	GLBA general record-keeping; business continuity; potential litigation hold considerations	Automated deletion from email and messaging platforms; secure deletion from archives

Data Category	Description & Examples	Classification	Retention Period	Legal / Business Justification	Disposal Method
	operations				
Backup & Disaster Recovery Data	Full and incremental backups of databases, file systems, and application data; disaster recovery snapshots and replication copies	Per source data classification	Follows source data retention period plus 90 days for backup cycle completion and verification	Business continuity and disaster recovery requirements; ISO 27001 Annex A.12.3	Cryptographic erasure of backup media; verified deletion from all backup storage locations and cloud snapshots
Marketing & Analytics Data	Anonymized and aggregated usage analytics, market research data, campaign performance metrics, and de-identified behavioral data	Internal	2 years from date of collection or generation	Business analytics and strategic planning; data must be fully de-identified per CCPA §1798.140(m) and cannot be re-identified	Standard deletion from analytics platforms; verification that no re-identification is possible

5.0 SECURE STORAGE REQUIREMENTS

5.1 Encryption at Rest

All data classified as Confidential or Restricted shall be encrypted at rest using the Advanced Encryption Standard (AES) with a minimum key length of 256 bits (AES-256). Encryption keys shall be managed through a dedicated Key Management Service (KMS) with hardware security module (HSM) backing where available. Key rotation shall occur at least annually, or immediately upon suspected compromise.

5.2 Encryption in Transit

All data transmissions, whether internal or external, shall be encrypted using Transport Layer Security (TLS) version 1.2 or higher. Deprecated protocols (SSL, TLS 1.0, TLS 1.1) are prohibited. Certificate management procedures shall ensure valid, unexpired certificates are in use at all times.

5.3 Plaid Access Token Storage

Plaid access tokens shall be subject to the following enhanced security requirements:

- Encrypted at the database column level using envelope encryption, whereby each token is encrypted with a unique Data Encryption Key (DEK), which is in turn encrypted by a Key Encryption Key (KEK) managed by the KMS;
- Stored exclusively in server-side, production-grade databases with encrypted storage volumes;

- Never stored in, transmitted to, or accessible from client-side code, frontend applications, browser local storage, cookies, session storage, or client-accessible API responses;
- Never written to application logs, debug logs, error tracking systems, monitoring dashboards, or any log aggregation platform; and
- Access restricted to the minimum set of application service accounts required for Plaid API operations, with all access events logged.

5.4 Database Security

All databases containing Confidential or Restricted data shall adhere to the following requirements:

- Encrypted storage volumes using AES-256 at the disk or volume level;
- Regular security patching within 30 days of critical patch release, and within 90 days for non-critical patches;
- Hardened configurations following CIS Benchmarks or vendor-specific security baselines;
- Network segmentation isolating database servers from public-facing networks;
- Automated vulnerability scanning on a monthly basis; and
- Documented and tested backup and recovery procedures.

5.5 Cloud Infrastructure

MG9 Group LLC shall utilize only cloud service providers that maintain current SOC 2 Type II certification (e.g., Amazon Web Services, Google Cloud Platform, Microsoft Azure). Cloud environments shall be configured with:

- Encryption enabled for all storage services (object storage, block storage, databases);

- Identity and access management (IAM) policies enforcing least privilege;
- Cloud audit logging enabled for all administrative actions; and
- Geographic data residency controls ensuring data remains within the United States unless otherwise required.

5.6 Data Segregation

End User Data obtained through Plaid integrations shall be logically separated from internal operational data. Logical separation shall be enforced through distinct database schemas, access control lists, or dedicated storage containers. Cross-environment data transfers (e.g., production to staging) are prohibited unless data is fully de-identified prior to transfer.

5.7 Backup Encryption

All backup media, including full backups, incremental backups, and disaster recovery snapshots, shall be encrypted using the same encryption standards applied to primary storage (AES-256). Backup encryption keys shall be managed independently from primary data encryption keys and stored securely in the KMS.

6.0 ACCESS CONTROLS

6.1 Role-Based Access Control

MG9 Group LLC implements Role-Based Access Control (RBAC) across all information systems. Access is granted based on the principle of least privilege, ensuring that each individual has access only to the data and systems necessary to perform their assigned duties. No individual shall be granted standing administrative or root-level access to production systems

without documented approval from the IT Security Manager and the Compliance Officer.

6.2 Multi-Factor Authentication

Multi-Factor Authentication (MFA) is required for all personnel accessing systems that contain Restricted or Confidential data. MFA shall employ at least two distinct authentication factors (e.g., something the user knows and something the user possesses). MFA shall also be required for all remote access connections, VPN sessions, and cloud management consoles.

6.3 Access Provisioning and Deprovisioning

Access provisioning shall follow a formal request and approval workflow documented in the Company's access management system. Upon role change, transfer, or termination, access shall be modified or revoked within 24 hours. For involuntary terminations, access shall be revoked immediately and concurrent with the separation event. All provisioning and deprovisioning actions shall be logged for audit purposes.

6.4 Quarterly Access Reviews

The Compliance Officer, in coordination with the IT Security Manager, shall conduct quarterly access reviews and recertification for all systems containing Confidential or Restricted data. Reviews shall verify that:

- All active accounts correspond to current, authorized personnel;
- Access levels are appropriate for each individual's current role and responsibilities;
- Privileged accounts are limited to the minimum number necessary; and
- Any anomalous or unauthorized access is identified, investigated, and remediated.

6.5 Privileged Access Management

Privileged accounts, including database administrator accounts, system administrator accounts, and security personnel accounts, shall be subject to enhanced controls including dedicated privileged access workstations, session recording for administrative actions on Restricted data systems, just-in-time (JIT) access provisioning where technically feasible, and separate credentials from standard user accounts.

6.6 Roles and Access Matrix

Role	Data Access Level	Systems Accessed	Approval Required
Chief Executive Officer	Restricted, Confidential, Internal, Public	All business systems; executive dashboards; compliance platforms; financial reporting systems	Board-level authorization; self-certification with Compliance Officer review
Compliance Officer / Data Protection Officer	Restricted, Confidential, Internal, Public	Compliance platforms; audit systems; data governance tools; Plaid dashboard; access management systems; incident management	CEO approval for Restricted access; self-certification for Confidential and below
Developer / Engineer	Confidential (production — read-only, via application layer); Internal; Public	Development environments; CI/CD pipelines; source code repositories; application monitoring;	IT Security Manager approval; Compliance Officer approval for production data access

Role	Data Access Level	Systems Accessed	Approval Required
		Plaid API (via application service accounts only)	
Customer Support	Confidential (limited to relevant customer records); Internal; Public	Customer relationship management (CRM) system; ticketing system; user account management (limited fields)	Compliance Officer approval; access limited to active case records
External Auditor	Confidential, Internal (read-only, time-limited)	Audit logs; compliance documentation; access review records; policy documentation; sampling of data controls	CEO and Compliance Officer joint approval; access provisioned for audit engagement period only; NDA required
Third-Party Vendor	As contractually specified (minimum necessary)	Limited to systems specified in Data Processing Agreement; vendor-specific service accounts only	Compliance Officer approval; CEO approval for Restricted data access; executed DPA required

7.0 DATA DISPOSAL AND DESTRUCTION PROCEDURES

7.1 General Disposal Requirements

Data disposal shall be initiated within 30 calendar days following the expiration of the applicable retention period specified in Section 4.0, unless

a legal hold or documented exception is in effect. All disposal activities shall be performed by authorized personnel and documented in the Company's disposal log.

7.2 Electronic Data Disposal

The following methods are authorized for disposal of electronic data, listed in order of preference:

- **Cryptographic Erasure (Preferred):** Permanent destruction of all copies of the encryption keys protecting the data, rendering the encrypted data irrecoverable. This method is preferred for large datasets, cloud-hosted data, and encrypted database records.
- **Secure Overwrite:** Overwriting data using methods compliant with NIST SP 800-88 Rev. 1 "Clear" or "Purge" guidelines, depending on the data classification level and media type. A minimum of one pass with verified overwrite is required for Clear; Purge requires technology-specific methods (e.g., block erase for SSDs, firmware-level secure erase for HDDs).

7.3 Plaid Access Token Disposal

Plaid access tokens shall be disposed of using the following mandatory procedure:

1. Programmatic revocation of the token via the Plaid API `/item/remove` endpoint, which terminates the connection between MG9 Group LLC and the end user's financial institution;
2. Deletion of the token value from the primary database, including any cached copies;
3. Verification that the token has been removed from all database replicas within 24 hours;

4. Removal from backup media within the 90-day backup cycle window; and
5. Logging of the revocation and deletion event with timestamp, method, and responsible party.

7.4 Database Record Disposal

Database records shall be securely deleted with post-deletion verification. Deletion must be propagated to all replicas, read replicas, and standby instances within 24 hours. Disposal from backup media shall be completed within 90 days through either targeted backup record removal or backup cycle expiration. Database vacuum or compaction operations shall be performed following bulk deletion operations to prevent data recovery from unallocated space.

7.5 Physical Media Disposal

Physical storage media (hard drives, solid-state drives, USB devices, tapes) shall be destroyed in accordance with NIST SP 800-88 Rev. 1 "Destroy" guidelines using one or more of the following methods:

- **Degaussing:** Application of a magnetic field sufficient to render magnetic media unreadable (HDDs and tapes only; not effective for SSDs);
- **Shredding:** Physical destruction of the media into particles of a size that precludes data recovery; or
- **Incineration:** Thermal destruction of the media at a licensed, certified destruction facility.

A Certificate of Destruction shall be obtained from the destruction vendor for all physical media disposal events and retained for a minimum of 3 years.

7.6 Paper Document Disposal

Paper documents containing Confidential or Restricted information shall be destroyed using cross-cut shredding at a minimum security level of DIN 66399 Level P-4 (particle size no greater than 2mm x 15mm). Documents classified as Internal may be disposed of using DIN 66399 Level P-3 cross-cut shredding.

7.7 Cloud Data Disposal

Data stored in cloud environments shall be deleted from all regions, availability zones, and data centers in which it resides. This includes deletion from:

- Primary storage (object storage buckets, block storage volumes, database instances);
- All automated snapshots and manual snapshots;
- Cross-region replication targets;
- Content delivery network (CDN) caches; and
- Cloud provider recycle bins or soft-delete recovery windows (explicit purge required).

Verification of cloud data deletion shall be documented, including confirmation from cloud provider audit logs where available.

7.8 Disposal Verification

All disposal of Restricted data shall be subject to two-person integrity verification, whereby two authorized individuals independently confirm that disposal was executed correctly and completely. For Confidential data, single-person verification with documented attestation is sufficient.

7.9 Disposal Documentation

All disposal actions shall be documented in the Company's data disposal log, which shall include the following for each disposal event:

- Date and time of disposal;
- Description of data disposed (category, classification, approximate volume);
- Disposal method used;
- Name(s) of responsible party(ies) who performed the disposal;
- Name(s) of verifier(s) (for Restricted data, two-person verification);
- Confirmation of successful completion; and
- Reference to any Certificate of Destruction (for physical media).

Disposal logs shall be retained for a minimum of 3 years following the disposal event.

8.0 DATA SUBJECT RIGHTS AND REQUESTS

8.1 Consumer Rights Under CCPA/CPRA

MG9 Group LLC recognizes and upholds the rights of California consumers (and consumers in other jurisdictions where applicable) to:

- **Right to Know:** Request disclosure of the categories and specific pieces of Personal Data collected, the sources of collection, the business purposes for collection, and the categories of third parties with whom data is shared;
- **Right to Delete:** Request deletion of Personal Data collected by MG9 Group LLC, subject to applicable legal exceptions;

- **Right to Correct:** Request correction of inaccurate Personal Data;
- **Right to Opt-Out:** Opt out of the sale or sharing of Personal Data; and
- **Right to Non-Discrimination:** Exercise any of the above rights without receiving discriminatory treatment.

8.2 Plaid-Specific Data Deletion Process

When an end user requests deletion of their data, MG9 Group LLC shall:

6. Verify the identity of the requesting party using a two-step verification process (confirmation of account ownership via registered email and secondary verification factor);
7. Revoke the associated Plaid access token(s) via the Plaid API to disconnect the user's financial institution accounts;
8. Delete all End User Data associated with the requesting user from primary databases;
9. Initiate deletion from backup media in accordance with Section 7.4;
10. Coordinate with Plaid to confirm that Plaid has been notified of the disconnection; and
11. Provide written confirmation of deletion to the requesting user within the response timeline.

8.3 Response Timeline

MG9 Group LLC shall respond to all verifiable consumer requests within 45 calendar days of receipt, in accordance with CCPA §1798.105. If additional time is required due to the complexity of the request or the volume of requests received, MG9 Group LLC may extend the response period by an additional 45 calendar days, provided that the consumer is notified of the extension and the reason for it within the initial 45-day period.

8.4 Verification Procedures

MG9 Group LLC shall verify the identity of all requestors before processing data subject requests. Verification shall include matching at least two data points provided by the requestor against information already maintained by MG9 Group LLC. For requests to delete Restricted data or requests made by authorized agents, enhanced verification including a signed declaration under penalty of perjury may be required.

8.5 Request Record Keeping

Records of all data subject requests and the Company's responses shall be maintained for a minimum of 24 months from the date of the request, in accordance with CCPA §1798.185 implementing regulations. Records shall include the request date, request type, requestor identity (verified), actions taken, response date, and any exceptions applied.

9.0 AUDIT AND COMPLIANCE MONITORING

9.1 Annual Internal Audit

The Compliance Officer shall conduct or commission a comprehensive internal audit of data retention compliance on an annual basis. The audit shall assess adherence to the retention schedules specified in Section 4.0, the effectiveness of disposal procedures, the accuracy of data classification, and the completeness of disposal documentation. Audit findings shall be reported to the Chief Executive Officer and documented with remediation timelines.

9.2 Quarterly Automated Scans

The IT Security Manager shall implement automated scanning processes to identify data that has exceeded its authorized retention period. Automated scans shall be executed at least quarterly and shall cover all production databases, file storage systems, backup repositories, and cloud storage environments. Data identified as exceeding retention periods shall be flagged for disposal and processed within 30 days of identification.

9.3 SOC 2 Type II Alignment

MG9 Group LLC shall maintain alignment with SOC 2 Trust Services Criteria and shall undergo an annual SOC 2 Type II assessment conducted by an independent, qualified auditor. The assessment shall cover the security, availability, and confidentiality trust service categories at a minimum. Audit reports shall be made available to Plaid and other authorized parties upon request.

9.4 Compliance Metrics and KPIs

The following key performance indicators shall be tracked and reported quarterly to the Chief Executive Officer:

- Percentage of data categories in compliance with defined retention periods;
- Average time between retention period expiration and confirmed disposal;
- Number and resolution time of data subject requests;
- Number of access review findings and remediation rate;
- Number of policy violations and corrective actions taken; and
- Completion rate of mandatory data retention training.

9.5 Annual Policy Review

This Policy shall be reviewed at least annually, or more frequently upon the occurrence of material regulatory changes, significant security incidents, changes to MG9 Group LLC's business operations, or updates to Plaid's Developer Policy or security requirements. All revisions shall be documented in the version history table and distributed to all applicable personnel.

9.6 Incident Reporting for Retention Violations

Any identified failure to comply with the retention schedules, disposal procedures, or access controls specified in this Policy shall be reported to the Compliance Officer within 24 hours of discovery. Violations shall be investigated, documented, and remediated in accordance with Section 11.0 of this Policy.

9.7 Plaid Compliance Readiness

MG9 Group LLC shall maintain a state of readiness for Plaid security reviews and compliance assessments at all times. This includes maintaining up-to-date documentation of data handling practices, retaining evidence of policy compliance (audit logs, access reviews, disposal records), and designating the Compliance Officer as the primary point of contact for Plaid compliance inquiries.

10.0 ROLES AND RESPONSIBILITIES

The following table defines the roles and responsibilities for data retention and disposal governance within MG9 Group LLC.

Role	Responsibilities
Chief Executive Officer (CEO)	Ultimate accountability for data governance and regulatory compliance across the organization Approval authority for this Policy and all material amendments Approval authority for policy exceptions jointly with the Compliance Officer Receipt and review of quarterly compliance metrics and annual audit reports Allocation of resources necessary for policy implementation and maintenance Escalation point for unresolved compliance issues
Data Protection Officer / Compliance Officer	Day-to-day oversight of policy implementation and enforcement Conduct or commission annual data retention compliance audits Manage and respond to data subject access, deletion, and correction requests Serve as the primary liaison for Plaid compliance reviews and regulatory inquiries Coordinate quarterly access reviews and recertification Maintain the data disposal log and retention schedule documentation Lead investigation and remediation of retention and disposal violations Develop and deliver data retention training programs Monitor regulatory changes and recommend policy updates Report compliance metrics and KPIs to the CEO on a quarterly basis
IT Security Manager	Implementation and maintenance of technical security controls (encryption, access management, logging) Management of the Key Management Service (KMS) and encryption key lifecycle Configuration and maintenance of automated retention scanning tools Execution of technical disposal

Role	Responsibilities
	procedures (cryptographic erasure, secure overwrite) Security patching and vulnerability management for data storage systems Maintenance of cloud infrastructure security configurations Technical support for access provisioning, deprovisioning, and MFA enrollment Incident response coordination for security events involving data stores
Development Team	Adherence to secure coding standards for all applications handling Confidential or Restricted data Implementation of Plaid API integration in compliance with Plaid Developer Policy Ensuring Plaid access tokens are never exposed in logs, client-side code, or frontend storage Implementation of automated data lifecycle management features within applications Participation in code reviews focused on data handling and token management Reporting any data handling anomalies or potential violations to the Compliance Officer
All Employees and Contractors	Compliance with this Policy and all related data handling procedures Completion of mandatory annual data retention and disposal training Prompt reporting of suspected policy violations, data breaches, or unauthorized data access to the Compliance Officer within 24 hours of discovery Proper classification of data created or received in the course of duties Secure handling and disposal of data in accordance with its classification level
External Auditors	Independent verification of data retention and disposal compliance during audit engagements

Role	Responsibilities
	Assessment of the effectiveness of technical and administrative controls Issuance of audit findings, recommendations, and remediation guidance Confidential handling of all Company data accessed during the audit

10.1 Reporting Structure and Escalation

The Compliance Officer reports directly to the Chief Executive Officer on all matters related to data governance, retention, and disposal compliance. The IT Security Manager reports to the Compliance Officer for policy compliance matters and to the CEO for organizational matters. Escalation of unresolved compliance issues shall follow the path: IT Security Manager → Compliance Officer → CEO. Issues involving potential regulatory violations or data breaches shall be escalated immediately to the CEO and Compliance Officer concurrently.

11.0 INCIDENT RESPONSE FOR DATA RETENTION VIOLATIONS

11.1 Definition of a Retention/Disposal Violation

A data retention or disposal violation is any event in which:

- Data is retained beyond its authorized retention period without a documented legal hold or approved exception;
- Data is disposed of before the expiration of its required retention period;

- Disposal is performed using a method that does not meet the requirements specified in Section 7.0;
- Disposal documentation is incomplete, inaccurate, or missing;
- Unauthorized individuals access data scheduled for or undergoing disposal;
- Plaid access tokens are not revoked or deleted upon user disconnection or account deactivation; or
- Data subject deletion requests are not fulfilled within the required timeline.

11.2 Reporting Procedures

Any individual who discovers or suspects a data retention or disposal violation shall report it to the Compliance Officer within 24 hours of discovery. Reports may be made via email, internal ticketing system, or direct communication. Reports shall include, at a minimum, a description of the suspected violation, the data category and classification involved, the systems affected, and the date and time of discovery.

11.3 Investigation and Remediation

Upon receipt of a violation report, the Compliance Officer shall:

12. Acknowledge receipt of the report within 4 business hours;
13. Assess the severity and scope of the violation within 24 hours;
14. Engage the IT Security Manager and other relevant personnel to contain and investigate the incident;
15. Determine the root cause of the violation;
16. Implement immediate corrective actions to remediate the violation;
17. Document all findings, corrective actions, and preventive measures; and

18. Close the incident with a written report to the CEO within 30 days of discovery.

11.4 Notification Requirements

If a retention or disposal violation results in unauthorized access to or disclosure of End User Data or Personal Data, the following notification obligations apply:

- **Affected Individuals:** Notification within 72 hours of confirming the breach, or as required by applicable state breach notification laws, whichever is sooner;
- **Regulatory Authorities:** Notification to applicable regulators (e.g., California Attorney General for CCPA, federal regulators for GLBA) within the timeframes prescribed by applicable law;
- **Plaid:** If the violation involves End User Data obtained through Plaid APIs or Plaid access tokens, Plaid shall be notified within 24 hours of confirming the incident, in accordance with Plaid's Developer Policy and any applicable contractual obligations; and
- **Law Enforcement:** As required by applicable law or as recommended by legal counsel.

11.5 Post-Incident Review

Following the closure of each violation incident, the Compliance Officer shall conduct a post-incident review within 30 days to identify systemic issues, assess the effectiveness of corrective actions, and implement preventive controls to reduce the likelihood of recurrence. Post-incident review findings shall be incorporated into the next quarterly compliance report and, where applicable, into updates to this Policy.

12.0 THIRD-PARTY AND VENDOR MANAGEMENT

12.1 Vendor Requirements

All third-party vendors, service providers, and subprocessors that access, process, store, or transmit MG9 Group LLC data classified as Internal or above shall be required to:

- Demonstrate compliance with security standards commensurate with the data classification level they handle;
- Maintain SOC 2 Type II certification or equivalent independent security assessment;
- Implement encryption, access controls, and disposal procedures consistent with this Policy;
- Cooperate with MG9 Group LLC audit and compliance monitoring activities; and
- Report any security incidents or data breaches involving MG9 Group LLC data within 24 hours of discovery.

12.2 Contractual Obligations

All vendor agreements involving access to Confidential or Restricted data shall include contractual provisions requiring:

- Defined data retention periods that do not exceed those specified in this Policy;
- Secure disposal of all MG9 Group LLC data upon contract termination or expiration, with written certification of disposal;
- Prohibition on secondary use of MG9 Group LLC data for purposes not authorized in the agreement;

- Right of MG9 Group LLC to audit vendor data handling practices; and
- Immediate notification of any subprocessor changes.

12.3 Annual Vendor Compliance Assessments

The Compliance Officer shall conduct annual compliance assessments of all vendors handling Confidential or Restricted data. Assessments shall include review of the vendor's current SOC 2 report or equivalent, verification of data handling and disposal practices, assessment of security controls, and evaluation of incident response capabilities. Vendors that fail to meet compliance requirements shall be placed on a remediation plan or replaced.

12.4 Data Processing Agreements

A Data Processing Agreement (DPA) shall be executed with each vendor that processes Personal Data or End User Data on behalf of MG9 Group LLC. Each DPA shall specify the nature and purpose of processing, the categories of data processed, the obligations of the processor, data retention and deletion requirements, sub-processing restrictions, and audit rights of MG9 Group LLC.

12.5 Plaid-Specific Obligations

MG9 Group LLC acknowledges its obligations as an authorized developer utilizing Plaid's services. In this capacity, MG9 Group LLC shall:

- Comply with all requirements of the Plaid Developer Policy regarding data access, use, retention, and disposal;
- Use End User Data only for the purposes disclosed to and authorized by the end user;
- Not sell End User Data obtained through Plaid;
- Maintain adequate security measures to protect Plaid access tokens and End User Data;

- Promptly respond to Plaid's requests for information regarding data handling practices; and
- Immediately notify Plaid of any security incident involving End User Data or Plaid access tokens.

13.0 TRAINING AND AWARENESS

13.1 Annual Training

All employees and contractors of MG9 Group LLC shall complete mandatory annual training on data retention and disposal policies and procedures. Training shall cover data classification, retention schedules, secure handling requirements, disposal procedures, data subject rights, and incident reporting obligations. Training shall be completed within 30 days of assignment and annually thereafter.

13.2 Role-Specific Training

Personnel in roles with direct access to Restricted or Confidential data, particularly developers and engineers working with Plaid API integrations, shall receive additional role-specific training covering:

- Secure handling of Plaid access tokens and API credentials;
- Proper implementation of encryption and access control mechanisms;
- Procedures for programmatic token revocation and data deletion;
- Secure coding practices for financial data applications; and
- Incident recognition and reporting for data handling anomalies.

13.3 New Hire Onboarding

All new employees and contractors shall complete data retention and disposal training as part of their onboarding process, no later than 14

calendar days from their start date. New hires shall not be granted access to Confidential or Restricted data until training is completed and acknowledged.

13.4 Training Records

Records of all training completions, including the trainee's name, training module, completion date, and assessment results (if applicable), shall be maintained by the Compliance Officer for a minimum of 3 years. Training records shall be available for review during internal and external audits.

14.0 POLICY ENFORCEMENT AND EXCEPTIONS

14.1 Enforcement

Compliance with this Policy is mandatory for all personnel within its scope. Violations of this Policy may result in disciplinary action, up to and including termination of employment or contract. The severity of disciplinary action shall be proportionate to the nature and impact of the violation, taking into account whether the violation was intentional or negligent, the sensitivity of the data involved, and the extent of any resulting harm.

14.2 Exception Process

Exceptions to the retention schedules or disposal requirements specified in this Policy may be granted only under the following conditions:

19. A written exception request is submitted to the Compliance Officer, detailing the specific policy provision for which an exception is sought, the business or legal justification, the proposed alternative measure, and the requested duration of the exception;

20. The exception is reviewed and jointly approved in writing by both the Chief Executive Officer and the Compliance Officer;
21. The approved exception is documented, including its scope, duration, conditions, and any compensating controls; and
22. The exception is reviewed quarterly and expires automatically if not renewed.

Exceptions shall not be granted if they would result in non-compliance with applicable laws, regulations, or the Plaid Developer Policy.

14.3 Legal Hold Procedures

When MG9 Group LLC receives notice of pending or anticipated litigation, regulatory investigation, or government inquiry, the Compliance Officer shall issue a legal hold notice that overrides the standard retention periods specified in this Policy for all data potentially relevant to the matter. Legal hold procedures include:

- Identification and preservation of all potentially relevant data;
- Notification to all custodians of relevant data of their obligation to preserve;
- Suspension of automated disposal processes for data subject to the hold;
- Periodic reminders to custodians during the hold period; and
- Release of the hold and resumption of standard retention schedules upon written authorization from legal counsel.

All legal hold actions shall be documented and retained for the duration of the hold plus 3 years.

14.4 Exception Register

The Compliance Officer shall maintain a register of all active exceptions, including the exception details, approval documentation, duration, and review dates. The exception register shall be reviewed quarterly by the Compliance Officer and CEO, and all expired or unnecessary exceptions shall be closed.

15.0 POLICY REVIEW AND UPDATES

15.1 Review Schedule

This Policy shall be reviewed and, if necessary, updated at least annually. In addition, an ad hoc review shall be conducted upon the occurrence of any of the following events:

- Material changes to applicable federal or state laws and regulations;
- Updates to the Plaid Developer Policy or security requirements;
- Significant changes to MG9 Group LLC's business operations, technology infrastructure, or data processing activities;
- Findings from internal or external audits that indicate policy deficiencies;
- Data security incidents that reveal gaps in the current policy; or
- Organizational changes that affect roles and responsibilities defined in this Policy.

15.2 Change Management

All proposed changes to this Policy shall be drafted by the Compliance Officer, reviewed by affected stakeholders, and approved by the Chief

Executive Officer prior to implementation. Material changes shall be communicated to all personnel within the scope of the Policy within 14 calendar days of approval. Changes shall be reflected in an updated version number and documented in the Version History table.

15.3 Distribution and Acknowledgment

The current version of this Policy shall be made available to all employees and contractors via the Company's internal document management system. All personnel shall be required to acknowledge receipt and understanding of this Policy and any material updates thereto. Acknowledgment records shall be maintained by the Compliance Officer.

APPENDICES

APPENDIX A: Data Retention Schedule Quick Reference

Data Category	Classification	Retention Period	Disposal Method
Plaid Access Tokens & API Credentials	Restricted	Active connection only; delete on disconnect	API revocation + cryptographic erasure
End User Financial Data	Confidential	3 years from collection or last activity	Cryptographic erasure
Identity Verification Data	Restricted	5 years from account closure or last verification	Cryptographic erasure; two-person verification
Transaction & Payment Records	Confidential	7 years from transaction date	Cryptographic erasure

Data Category	Classification	Retention Period	Disposal Method
User Account Data	Confidential	Account duration + 1 year post-closure	Secure database deletion
Audit Logs & Security Logs	Confidential	3 years minimum	Secure deletion
Consent Records	Confidential	7 years from consent date	Secure deletion with audit trail
API Request/Response Logs	Internal	1 year from request date	Automated log rotation
Employee & Contractor Records	Internal	Employment duration + 7 years	Cross-cut shredding (paper); secure deletion (electronic)
Business Communications	Internal	3 years from date of communication	Automated platform deletion
Backup & Disaster Recovery Data	Per source	Source retention + 90 days	Cryptographic erasure of backup media
Marketing & Analytics Data	Internal	2 years from collection	Standard deletion

APPENDIX B: Disposal Verification Checklist

The following checklist shall be completed for each disposal event involving Confidential or Restricted data:

☐	Checklist Item
☐	Retention period expiration confirmed against Section 4.0 schedule
☐	No active legal hold applies to this

☐	Checklist Item
	data (confirmed with Compliance Officer)
☐	No pending or open data subject requests relate to this data
☐	Data classification level verified
☐	Disposal method is appropriate for data classification per Section 7.0
☐	For Plaid access tokens: Token revoked via Plaid API prior to deletion
☐	Data deleted from primary storage
☐	Data deleted from all replicas and read replicas (within 24 hours)
☐	Backup deletion initiated (completion within 90 days)
☐	Cloud snapshots and cross-region copies deleted (if applicable)
☐	Disposal verified by authorized party (two-person verification for Restricted data)
☐	Certificate of Destruction obtained (physical media only)
☐	Disposal log entry completed with all required fields
☐	Post-disposal verification scan confirms data is unrecoverable

Disposal Performed By: _____ Date: _____

Disposal Verified By: _____ Date: _____

Compliance Officer Sign-Off: _____ Date: _____

APPENDIX C: Applicable Laws and Regulations Reference

Law / Regulation / Standard	Relevance to Data Retention	Key Provisions
Gramm-Leach-Bliley Act (GLBA)	Governs collection, disclosure, and protection of consumers' nonpublic personal information by financial institutions	Safeguards Rule (16 CFR Part 314); Privacy Rule (Regulation P, 12 CFR Part 1016); record-keeping for privacy notices and opt-out records
California Consumer Privacy Act / California Privacy Rights Act (CCPA/CPRA)	Consumer rights regarding Personal Data; data minimization and retention requirements	Right to delete (§1798.105); Right to know (§1798.110); data retention disclosure (§1798.100); 45-day response requirement; 24-month request record retention
Consumer Financial Protection Bureau (CFPB) Regulations	Consumer financial data protections and complaint handling	Complaint retention (3 years minimum); consumer data access and portability requirements; Section 1033 open banking rules
Sarbanes-Oxley Act (SOX)	Financial record integrity and retention for publicly relevant financial records	Section 802: 7-year retention for audit work papers and financial records; criminal penalties for document destruction during investigations
Bank Secrecy Act / Anti-Money Laundering (BSA/AML)	Record-keeping for identity verification and suspicious activity	31 CFR §1010.430: 5-year retention for CDD/KYC records; Suspicious Activity Reports (SARs); Currency Transaction Reports (CTRs)

Law / Regulation / Standard	Relevance to Data Retention	Key Provisions
Internal Revenue Code (IRC) §6501	Tax record retention for statute of limitations compliance	3-year general statute; 6-year extended statute for substantial omissions; 7-year recommended retention for comprehensive coverage
NIST SP 800-88 Rev. 1	Guidelines for media sanitization and data disposal	Clear, Purge, and Destroy sanitization methods; media-specific guidance; verification requirements; documentation requirements
SOC 2 Trust Services Criteria	Security, availability, confidentiality, processing integrity, and privacy controls	CC6.1 (logical and physical access); CC7.2 (system monitoring); CC6.5 (data disposal); CC6.7 (data transmission); audit trail requirements
ISO 27001:2022 / ISO 27701:2019	Information security and privacy management system requirements	Annex A.8.10 (information deletion); Annex A.12.4 (logging and monitoring); Annex A.12.3 (backup); privacy information lifecycle management
Plaid Developer Policy	Requirements for authorized developers accessing Plaid APIs	User consent and authorization; data use limitations; token security; data deletion obligations; security incident notification; compliance with applicable laws

APPENDIX D: Document Acknowledgment Form

I, the undersigned, acknowledge that I have received, read, and understand the MG9 Group LLC Data Retention and Disposal Policy (Version 1.0, effective April 22, 2026). I agree to comply with all provisions of this Policy in the performance of my duties. I understand that violations of this Policy may result in disciplinary action, up to and including termination of employment or contract.

Employee / Contractor Name (Print):

_____

Title / Role: _____

Department: _____

Signature

Date: _____

Witnessed By (Compliance Officer):

Signature

Data Protection Officer / Compliance Officer

Date: _____

This acknowledgment form shall be retained by the Compliance Officer for a minimum of 3 years following the termination of the signatory's relationship with MG9 Group LLC. Return the completed form to the Compliance Officer within 14 calendar days of receipt.

POLICY APPROVAL

This Data Retention and Disposal Policy has been reviewed and approved by the undersigned on the date indicated below.

Chief Executive Officer

MG9 Group LLC

Date: April 22, 2026

Data Protection Officer / Compliance Officer

MG9 Group LLC

Date: April 22, 2026

— End of Document —