MELA FINANCE INC. — GLOBAL PRIVACY POLICY

Effective Date: 9 May 2025

TABLE OF CONTENTS

---

1 | ABOUT THIS POLICY

Mela Finance Inc. ("**Mela**," "**we**," "**our**," or "**us**") is a Delaware-incorporated neobank that offers global U.S.-dollar accounts, debit cards, and related services through partnerships with multiple U.S. chartered banks ("**Bank Partners**").

This Policy explains how we collect, use, disclose, and protect personal information when you:

- Use the **Mela** mobile application;
- Visit **www.mela.finance** or any website linking to this Policy;
- Communicate with our call-center, APIs, or other online/offline channels.

Each Bank Partner provides its own legally required privacy notice for the deposit or credit account it holds. Mela's Policy governs our independent data practices and applies globally, subject to additional regional rights found in Section 16.

We comply with, at minimum:

- **U.S. Federal**: Gramm-Leach-Bliley Act (GLBA), CFPB Regulation P, Bank Secrecy Act (BSA/AML), OFAC, Right to Financial Privacy Act, PCI-DSS v4.0.
- **U.S. State**: California CPRA, Virginia CDPA, Colorado CPA, and similar.
- **International**: EU & UK GDPR, Canada PIPEDA, Nigeria NDPR, and other local statutes where users reside.

---

2 | INFORMATION WE COLLECT

2.1 Categories of Personal Information

Category	Typical Data Elements	Source(s)
Identifiers	Name, aliases, date of birth, SSN/passport/TIN, mailing & billing addresses, email, phone	You; KYC vendors
Sensitive Identifiers	Biometric facial templates & liveness video, PINs, mother's maiden name	You; device; Onfido
Financial & Transaction	Account & routing numbers, tokenized card PAN, balances, ACH/wire data, Plaid-sourced transactions, remittance details, merchant category codes	Charter banks; Plaid; payment networks
Device & Technical	OS/build, browser, app version, IP address, device ID, advertising ID, crash logs, locale, accessibility settings, motion/gyroscope data, battery/storage metrics	Device; SDKs
Location	GPS coordinates (if enabled), IP-based geolocation, time-zone	Device; IP lookup
Internet/Network Activity	Page views, clicks, referral URLs, session duration, cookies/pixels, heatmaps	Browser/app; analytics providers
Employment/Business	Employer name, EIN, occupation, income proofs, business registration docs	You; payroll APIs
Communications	Email content, chat transcripts, voice calls, voicemail, screen recordings (with notice)	You; support platform
Inferences & Profiles	Risk scores, behavioral biometrics, credit-builder metrics, marketing segments	Derived internally

2.2 Information You Provide to Us

You supply Personal Information when you:

- Download the app and create an account;
- Complete identity verification or upload documents;
- Link external bank or wallet accounts via Plaid;

- Contact support, engage on social media, enter promotions, or respond to surveys.

2.3 Information from Third Parties

We obtain data from:

- **Onfido** (identity & document verification, biometric liveness);
- **Plaid** (financial-account aggregation, balance & transaction pulls);
- **Credit bureaus & sanctions lists** (fraud, AML, KYC);
- **Payment networks & processors** (card authorization, disputes, chargebacks);
- **Marketing & attribution platforms** (subject to consent).

2.4 Cookies & Similar Technologies

We and our partners use:

- **Essential cookies/SDK events** – authentication, load balancing, fraud defence;
- **Analytics cookies (e.g., GA4, Mixpanel)** – usage metrics, A/B testing;
- **Advertising cookies/pixels (e.g., Meta, Google Ads, Adjust)** – only after opt-in, to measure campaign effectiveness.

You can manage preferences via our cookie banner (where required), in-app settings, browser controls, or OS-level privacy features (“Limit Ad Tracking,” “ATT”).

2.5 Technical & Device Data

Our mobile SDKs capture: accelerometer/gyroscope readings (to detect jailbreaks/emulators), network type, carrier, device language, accessibility status, crash diagnostics, and push-token IDs.

---

3 | HOW WE USE YOUR INFORMATION

Purpose	Examples

Account Opening & KYC	Verify identity, run PEP/sanctions screening, prevent duplicate accounts.
Provide Services	Maintain USD account, execute deposits/withdrawals, issue & manage debit cards, deliver statements, facilitate remittances, enable budgeting tools.
Fraud & Security	Biometric liveness checks, device fingerprinting, velocity checks, transaction monitoring, compromised credential screening.
Regulatory Compliance	BSA/AML reporting, OFAC & 314(b) screening, CTR/SAR filings, IRS/FATCA reporting, GDPR/CPRA rights fulfilment.
Customer Support	View account details, troubleshoot errors, resolve disputes, record calls as permitted.
Product Analytics	Measure feature adoption, perform cohort analysis, debug crashes, optimize UX.
Marketing & Personalization	Send tailored offers, referral programs, spend insights, only if you have not opted out.
Corporate Events	Due diligence for mergers, acquisitions, financing, or reorganization.

---

4 | LEGAL BASES FOR PROCESSING (GDPR)

Where GDPR or equivalent law applies, Mela operates as the **data controller** and relies on:

- **Contractual necessity** – to deliver requested Services;
- **Legal obligation** – AML, tax, consumer-protection laws;
- **Legitimate interests** – security, fraud prevention, product improvement;
- **Consent** – biometrics, precise geolocation, marketing communications.

---

5 | HOW WE SHARE YOUR INFORMATION

Recipient	Reason / Safeguards
Bank Partners	To open & service deposit/card/credit accounts. Governed by GLBA & bank privacy notices.
Service Providers (contract-bound)	Identity verification (Onfido), account aggregation (Plaid), payment processing, cloud hosting, cybersecurity, analytics, customer-support SaaS.
Card Networks & Payment Rails	Transaction authorization, settlement, dispute handling. Tokenization used where possible.
Regulators & Law-Enforcement	Subpoenas, court orders, SAR/CTR filings, audits, or to protect rights, property, and safety.
Professional Advisers	Auditors, lawyers, consultants under NDA for compliance or corporate governance.
Corporate Successors	Data transferred during M&A, financing, or insolvency—subject to this Policy.
Your Direction or Consent	Payments to a new payee, data portability requests, API integrations you enable.

We do not sell or rent Personal Information for monetary consideration and do not share it with third parties for their independent direct marketing.

---

6 | HOW WE SECURE YOUR INFORMATION

- **Encryption** – TLS 1.3 in transit; AES-256/GCM at rest; field-level encryption for PAN & SSN.
- **Access Controls** – Role-based (RBAC); hardware security keys & FIDO2 MFA; quarterly access-review attestations.
- **Network Security** – Segmented VPCs, WAF, DDoS protection, zero-trust infrastructure, weekly vulnerability scans, annual penetration tests.
- **PCI-DSS Compliance** – Card data isolated in PCI environment; SAQ-D maintained; ASV scans and ROC annually.
- **SOC 2 Type II & ISO 27001** – Independent audits of security, availability, confidentiality.

- **Incident Response** – 24×7 SOC, Playbooks aligned to NIST SP 800-61; user & regulator notification within 72 hours of a notifiable breach.

- **Employee Controls** – Background checks, mandatory security training, least-privilege principle, privacy confidentiality agreements.

---

7 | DATA RETENTION & DELETION

Data Type	Retention Rule
Customer identification records	≥5 years after account closure (BSA 31 CFR §1010.430).
Transaction & ledger data	≥5 years (BSA) or longer if dispute/litigation.
Call & chat recordings	2 years (or local statutory minimum).
Device/log data	90 days, unless tied to fraud/SOC investigation.
Marketing consents & opt-outs	Life of account + 4 years (FTC – CAN-SPAM safe-harbor).

On expiry, data is irreversibly anonymized or securely deleted (NIST SP 800-88).

---

8 | YOUR CHOICES & RIGHTS

- **Access / Portability** – Obtain a copy of Personal Information in a machine-readable format.

- **Correction** – Update inaccurate or incomplete data.

- **Deletion / Erasure** – Request deletion where no legal basis requires retention.

- **Restriction / Objection** – Limit or object to certain processing (GDPR).

- **Marketing Opt-Out** – Toggle in-app, click “unsubscribe,” or reply STOP to SMS.

- **Biometric & Location Consent** – Revoke at any time in device settings.

8.1 How to Exercise Your Rights

Submit in-app via **Settings › Privacy**, email **privacy@mela.finance**, or call **+1-833-MELA-DAT**. We verify identity (government ID + selfie match or 2FA) before actioning. Standard response times:

- 30 days (GDPR, GLBA);
- 45 days (CPRA, extendable once).

Denials include the legal basis and appeal instructions. Exercising rights never affects pricing or service levels.

---

9 | CHILDREN'S PRIVACY

Services are **not directed to children under 13** (or under the minimum age in your jurisdiction). We do not knowingly collect data from minors. If we discover such data, we delete it and disable the account unless a parent/guardian provides verifiable consent.

---

10 | INTERNATIONAL DATA TRANSFERS

Data may be processed in the U.S. or other countries with adequate safeguards:

- **EU/UK → U.S.** – EU-U.S. & UK-U.S. Data Privacy Framework or Standard Contractual Clauses.
- **Canada** – Contracts meeting PIPEDA Sch. 1.
- **Other** – Contractual clauses, binding corporate rules, or explicit consent as required.

---

11 | AUTOMATED DECISION-MAKING & PROFILING

Automated models (e.g., fraud risk, transaction monitoring, credit eligibility) are audited for fairness and accuracy. Where law grants the right, you may request human review and contest automated outcomes.

---

12 | THIRD-PARTY LINKS

Our app and website may contain links to third-party sites (e.g., partner offers, educational resources). Mela is **not responsible** for their privacy practices. Review those policies before sharing data.

---

13 | ACCESSIBILITY STATEMENT

We are committed to WCAG 2.1 AA compliance. If you require the Policy in an alternative format, email **accessibility@mela.finance** or call the support number above.

---

14 | UPDATES TO THIS POLICY

We may revise this Policy for legal, technical, or business reasons. Material changes will be announced by:

1. In-app banner or push notification;
2. Email, SMS, or phone (if materially impacting rights);
3. Updating the “Effective Date.”

Continuing to use the Services after notice constitutes acceptance of the revised Policy.

---

15 | CONTACT US

General Support: support@mela.finance
Privacy/Data Protection Officer: privacy@mela.finance
Legal Affairs: legal@mela.finance
Mail:

Mela Finance Inc.
8 The Green, Suite [Number]
Dover, DE 19901, USA

Unresolved complaints may be directed to the CFPB, your state Attorney-General, or your local Data Protection Authority.

---

16 | REGION-SPECIFIC ADDENDA

16-A California Privacy Notice (CPRA)

Under the California Consumer Privacy Rights Act (Cal. Civ. Code §1798.100 et seq.):

- **No Sale or Share**: Mela does **not** sell or share Personal Information as defined by CPRA.
- **Categories Collected (12 months)**: Identifiers; sensitive IDs; financial data; geolocation; Internet activity; inferences; device data; employment info.
- **Sensitive Data Use**: Strictly for KYC/AML, fraud prevention, and account servicing.
- **Right to Limit/Opt-Out**: Because we do not use sensitive data for inferring characteristics, CPRA §1798.121 right to limit does not apply.
- **How to Submit Requests**: See Section 8.1.

16-B EU/EEA & UK GDPR Addendum

- **Data Controller**: Mela Finance Inc., address above.
- **EU Representative (Art. 27 GDPR)**: [Name, Address, Email].
- **UK Representative (UK GDPR §27)**: [Name, Address, Email].
- **Supervisory Authority**: You have the right to lodge a complaint with your local DPA (e.g., ICO in UK, DPC in Ireland).
- **Legal Bases**: As outlined in Section 4.
- **Data Protection Impact Assessments**: Conducted for high-risk processing (biometrics, automated profiling).