Anti-Money Laundering (AML) Program

Radd Payment Solutions

47 Pleasant Street
Northampton, Massachusetts
www.raddpayments.com

---

1. Purpose

The purpose of this Anti-Money Laundering (AML) Program is to ensure that **Radd Payment Solutions ("Radd")** maintains effective policies, procedures, and internal controls designed to detect and prevent the use of its payment infrastructure for:

- Money laundering
- Terrorist financing
- Fraud
- Sanctions violations
- Other illicit financial activities

Radd recognizes that its services — which include payment processing, revenue stream assignment, billing management, and transaction aggregation — operate within regulated financial ecosystems. As such, Radd maintains an AML program consistent with expectations under the **Bank Secrecy Act (BSA)** and related regulations enforced by the **Financial Crimes Enforcement Network (FinCEN)**.

The program is designed to:

- Protect the integrity of the U.S. financial system
- Protect Radd's payment partners and financial institutions
- Ensure compliance with federal AML standards
- Mitigate financial crime risk across all payment channels managed by Radd

---

2. Scope

This AML Program applies to:

- All employees of Radd Payment Solutions
- All subsidiaries or special purpose entities controlled by Radd
- All client merchants whose revenue streams are managed by Radd
- All payment channels operated or facilitated by Radd

Including but not limited to:

- Credit card processing
- ACH and e-check payments
- Online platform revenue
- Recurring billing systems
- Direct B2B invoicing
- Subscription billing programs
- Platform-based commerce integrations

---

3. AML Governance & Oversight

Radd maintains a governance structure designed to ensure effective AML oversight.

AML Compliance Officer

Radd designates an **AML Compliance Officer** responsible for administering and enforcing this AML Program.

Responsibilities include:

- Oversight of AML policies and procedures
- Monitoring transaction activity
- Investigating suspicious activity
- Coordinating with financial institutions
- Ensuring compliance with regulatory obligations
- Training employees on AML responsibilities
- Maintaining AML documentation and audit readiness

The AML Compliance Officer reports directly to executive leadership.

---

4. Risk-Based AML Framework

Radd utilizes a **risk-based approach** to AML compliance.

This framework evaluates risk across the following categories:

Merchant Risk

Risk factors include:

- Businesses in financial distress
- Businesses undergoing restructuring
- High transaction volumes
- Rapid increases in payment activity
- Businesses operating in historically high-risk sectors

Geographic Risk

Radd evaluates exposure to:

- High-risk jurisdictions
- Sanctioned countries
- Regions associated with elevated financial crime risk

Payment Channel Risk

Certain payment channels carry increased risk, including:

- Card-not-present transactions
- Online platform transactions
- Cross-platform payment aggregation
- Third-party marketplace settlements

Transaction Risk

Transactions are monitored for indicators such as:

- Unusual transaction volume spikes
- Structured payments
- Abnormal refund patterns
- Rapid merchant onboarding followed by large processing volumes
- Payment flows inconsistent with merchant business models

---

5. Customer Identification Program (CIP)

Prior to onboarding any client or merchant, Radd performs identity verification procedures consistent with industry best practices.

Required information includes:

- Legal business name
- Employer Identification Number (EIN)
- Formation documents
- Beneficial ownership information
- Government-issued identification for controlling parties
- Business address verification
- Bank account verification

Radd may also obtain:

- Articles of incorporation
- Operating agreements
- Business licenses
- Ownership structure documentation
- Verification of restructuring advisors or consultants

Failure to provide required documentation may result in **denial or termination of services**.

---

6. Know Your Customer (KYC)

Radd conducts due diligence to understand the nature of each client's business operations.

KYC review includes:

- Description of business activity
- Expected payment volumes
- Payment methods utilized
- Industry classification
- Customer base profile
- Geographic markets served
- Historical financial activity (when available)

Clients whose business models are inconsistent with disclosed operations may be rejected.

---

7. Beneficial Ownership Identification

Radd collects beneficial ownership information for all entities onboarded.

This includes identifying individuals who:

- Own **25% or more** of the legal entity
- Exercise significant managerial control

Information collected includes:

- Full legal name
- Date of birth
- Address
- Identification number (SSN or passport)

---

8. Sanctions Screening

Radd screens all clients and beneficial owners against sanctions lists maintained by the **Office of Foreign Assets Control (OFAC)**.

Screening occurs:

- At onboarding
- Periodically during the relationship
- Upon changes to ownership structure

If a potential sanctions match is identified:

- Accounts will be frozen
- Transactions halted
- Relevant authorities and banking partners notified

---

9. Transaction Monitoring

Radd monitors payment activity processed through its systems for suspicious behavior.

Monitoring includes:

- Transaction velocity analysis
- Volume threshold alerts
- Refund and chargeback monitoring
- Rapid account activity increases
- Abnormal cross-platform revenue routing

Automated alerts and manual review processes are used to evaluate activity.

---

10. Suspicious Activity Reporting

If suspicious activity is detected, Radd will escalate internally for investigation.

Examples include:

- Structured transactions designed to evade reporting thresholds
- Payments inconsistent with stated business activity
- Sudden large payment spikes without explanation
- Payment activity involving sanctioned jurisdictions
- Rapid movement of funds through multiple accounts

If required, Radd will cooperate with its banking partners to facilitate reporting obligations.

Financial institutions ultimately determine whether to file **Suspicious Activity Reports (SARs)** with FinCEN.

---

11. Recordkeeping

Radd maintains records related to AML compliance for a minimum of **five (5) years**.

Records maintained include:

- Client onboarding documentation
- Identity verification materials
- Beneficial ownership information
- Transaction records
- Monitoring alerts
- Internal investigation documentation
- Compliance communications with banking partners

---

12. Employee Training

Radd provides AML training to all employees whose roles involve:

- Client onboarding
- Payment processing
- Financial reconciliation
- Client account management

Training includes:

- Identifying suspicious transactions
- Escalation procedures
- AML reporting responsibilities
- Sanctions awareness
- Fraud indicators

Training occurs:

- At onboarding
- Annually thereafter

---

13. Independent Review

Radd's AML program will be independently reviewed at least **once every two years**.

Reviews may be conducted by:

- Independent compliance consultants
- Legal advisors
- Qualified third-party auditors

Reviews assess:

- Effectiveness of AML policies
- Compliance with regulatory expectations
- Adequacy of transaction monitoring
- Staff training effectiveness

---

14. Program Updates

This AML Program will be reviewed and updated periodically to address:

- Changes in regulatory requirements
- Expansion of Radd's services

- New payment channels
- Emerging financial crime risks

---

15. Enforcement

Violation of this AML policy by employees or contractors may result in:

- Disciplinary action
- Termination
- Reporting to relevant authorities if required

---

16. Policy Approval

This Anti-Money Laundering Program has been approved by the executive leadership of **Radd Payment Solutions** and is effective immediately.

Approved By

President
Radd Payment Solutions

Chief Operating Officer
Radd Payment Solutions

Date: ___________________