Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Policy

Definitions

- “Company”, “we”, “our”, “PawPayments” - PawPayments, Inc.
- “Platform” - PawPayments’ cryptocurrency-only payment gateway and any related services.
- “User” - Any natural or legal person that uses the Platform.
- “Safelement Limited” - Our appointed third-party provider of AML (Anti-Money Laundering) and KYC (Know Your Customer) services (hereafter the “AML provider” or “KYC provider”). It is referenced once here; all subsequent references use “AML provider” or “KYC provider” as appropriate.

1. Introduction and Purpose

PawPayments is committed to preventing money laundering, terrorist financing, and other illicit activity conducted through its cryptocurrency services. This Policy explains the risk-based controls we apply in line with:

- Canada’s Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and regulations.
- Financial Action Task Force (FATF) Recommendations for virtual-asset service providers.
- Comparable international best practices (e.g., the EU 5th AML Directive, U.S. Bank Secrecy Act).

Because we process only virtual-currency transactions, our controls focus on blockchain-based risks; nevertheless, the core principles of AML/CTF apply. The Policy applies to every employee, officer, contractor, and all Users of the Platform.

2. Governance and Oversight

- Compliance Officer - PawPayments has designated an AML Compliance Officer with independent authority to design, maintain, and enforce this program, escalate issues to senior management, and liaise with regulators or law-enforcement agencies.
- Risk-Based Approach - Controls, resources, and monitoring intensity are allocated according to the inherent risk of each User, geography, and transaction.

3. Customer Due Diligence (CDD)

3.1. Basic On-Boarding

- Individuals: name, email, and other basic information; email/phone verification.
- Businesses: legal name, registration data, address, and account administrator details.

3.2. Tiered KYC

- Simplified due diligence for low-risk, low-volume activity.
- Enhanced Due Diligence (EDD) when triggers occur (e.g., high cumulative volume, large single transactions, blockchain flags, suspicious patterns).

3.3. Verification via AML provider

When EDD is required, Users complete identity verification through the AML provider, which performs document authentication, biometric checks, sanctions and PEP screening, and provides pass/fail results to our Compliance team. Refusal or failure results in denied or restricted service.

3.4. Business Clients

We identify beneficial owners (≥ 25 % ownership), directors, and controllers, and may request proof of business activities for high-risk clients.

3.5. Ongoing Monitoring

We re-verify identities when risk profiles change, conduct adverse-media checks, and screen against updated sanctions lists.

3.6. Prohibited Users

We do not provide services to:

- Persons or entities on relevant sanctions lists (UN, OFAC, EU, etc.).
- Users in jurisdictions subject to comprehensive sanctions or extremely high AML risk (e.g., North Korea, Iran).
- Identified accounts are terminated or frozen in accordance with legal requirements.

4. Transaction Monitoring and Risk Management

4.1. **Blockchain Analytics** - Automated screening of wallet addresses and transactions to detect links to darknet markets, mixers, ransomware, sanctioned addresses, or other illicit indicators.

4.2. **Velocity & Pattern Checks** - Thresholds for volume and frequency, detection of structuring or rapid in-and-out transfers.

4.3. **Geographic Risk** - Heightened scrutiny for transactions involving high-risk jurisdictions.

4.4. **Review of Flagged Transactions** - Transactions that trigger rules are paused where possible. The User may be contacted for source-of-funds information and, if not yet verified, must complete KYC with the AML provider.

4.5. **Suspicious Transaction Reports (STR/SAR)** - If there are reasonable grounds to suspect money laundering or terrorist financing, the Compliance Officer files a report with FINTRAC or the appropriate authority and documents the reasoning.

4.6. **Zero-Tolerance for Evasion** - Attempts to circumvent controls (multiple accounts, transaction splitting) are considered suspicious and can lead to account closure.

5. Record-Keeping

We retain for at least five years:

- KYC records and verification results.
- Detailed transaction data (date/time, amount, currency, addresses, hashes, associated Users).
- Investigation notes and STR/SAR filings.
- Compliance training logs and audit reports.

Records are stored securely with appropriate access controls.

6. Employee Training and Accountability

- Mandatory AML training for relevant staff at onboarding and annually thereafter.
- Content covers money-laundering typologies, red-flag indicators, legal obligations, and internal reporting procedures.
- Employees acknowledge understanding of the Policy and are subject to disciplinary action for non-compliance.
- Background checks for employees in sensitive roles help safeguard program integrity.

7. Sanctions and Anti-Fraud Controls

- All Users and transactions are screened against Canadian, UN, U.S., EU, and other applicable sanctions lists.
- Fraud monitoring overlaps with AML efforts; confirmed fraudulent activity results in frozen or cancelled transactions and potential law-enforcement referrals.
- PawPayments does not allow anonymous or fictitious-name accounts once risk thresholds are reached.

8. Program Review and Continuous Improvement

- The Compliance Officer reviews this Policy at least annually and after material regulatory changes.
- Independent audits of the AML program are conducted periodically; findings are remediated promptly.
- Version control is maintained, and significant updates are communicated to Users when relevant.
- PawPayments cooperates fully with regulators and law-enforcement agencies.

9. Conclusion

Preventing misuse of our Platform is integral to PawPayments' mission. All employees must understand and adhere to this Policy, and Users agree to its principles by accessing the Platform. A public version is available on our website. For questions, contact the Compliance Officer at **legal@pawpayments.com**.

By staying vigilant and applying a robust, risk-based AML/CTF framework, PawPayments safeguards its Users, its business, and the wider financial ecosystem.