

Anti-Money Laundering and Counter-Terrorist Financing Policy

Effective as of November 11, 2025

This Anti-Money Laundering and Counter-Terrorist Financing Policy (hereinafter "AML/CFT Policy") outlines the measures implemented by ARTCLUB 88 FINANCE CORPORATION (operating as ArtPay) to comply with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), S.C. 2000, c. 17, and associated Regulations, as administered by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). As a registered Money Services Business (MSB) dealing in virtual currency exchanges (P2P buying/selling of USDT/USDC with fiat currencies such as USD, EUR, CAD, GBP), we are committed to preventing money laundering (ML), terrorist financing (TF), and sanctions evasion.

Registered as Money Services Business (MSB) with FINTRAC (Canada)

MSB Number: M23048467

Legal Name: ARTCLUB 88 FINANCE CORPORATION

Operating Name: ArtPay

Incorporation Number: BC1443242

Definitions

Definitions used in this AML/CFT Policy:

ML/TF

Money Laundering / Terrorist Financing

AML/CFT

Anti-Money Laundering / Counter-Terrorist Financing

Client / Customer / Partner

An individual or legal entity receiving services from ARTCLUB 88 FINANCE CORPORATION, including P2P cryptocurrency exchanges.

PCMLTFA

Proceeds of Crime (Money Laundering) and Terrorist Financing Act, S.C. 2000, c. 17, as amended.

Regulations

Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations, SOR/2002-184, as amended.

FINTRAC

Financial Transactions and Reports Analysis Centre of Canada, the federal agency responsible for administering and enforcing the PCMLTFA.

STR

Suspicious Transaction Report, submitted to FINTRAC for suspected ML/TF activities.

EFT

Electronic Funds Transfer, including international transfers of \$10,000 CAD or more.

VC

Virtual Currency, such as USDT/USDC, subject to specific reporting and travel rule requirements.

Financial Services

Any banking, credit, investment, or payment services provided by the company, including P2P exchanges of virtual currency for fiat currencies.

Money Laundering

Any act or attempted act to disguise the source of money or assets derived from criminal activity, including converting, transferring, acquiring, possessing, or using property knowing it is derived from crime, or assisting in evading consequences. This applies regardless of whether the activity occurs in Canada or abroad.

Terrorist Financing

Providing or collecting property intending or knowing it will be used for terrorist activities.

Transaction

Any dealing involving the exchange, transfer, or disposition of funds or virtual currency. Related transactions are aggregated for reporting thresholds.

Business Relationship

A relationship established when a client opens an account or conducts two or more transactions requiring identity verification within a specified period.

Suspicious Transaction

A transaction or attempted transaction where there are reasonable grounds to suspect it is related to ML/TF, based on anomalies, client behavior, or other indicators.

Politically Exposed Person (PEP)

a) A person who holds or has held a prominent public function in Canada or abroad (e.g., head of state, senior politician, senior government/judicial/military official, senior executive of a state-owned corporation, important political party official).

b) A close associate or family member of such a person.

c) Includes foreign, domestic, and heads of international organizations (HIOs).

Beneficial Owner

The natural person(s) who ultimately owns or controls 25% or more of a legal entity, or exercises control through other means.

Identification Document

A government-issued document (e.g., passport, driver's license, provincial health card where permitted) that includes name, photo, signature, and is valid.

High-Risk Jurisdiction

Countries identified by FATF as high-risk or with strategic deficiencies in AML/CFT regimes, or subject to Canadian sanctions.

1. General Provisions

1.1. This AML/CFT Policy establishes procedures to detect, prevent, and mitigate ML/TF risks in compliance with the PCMLTFA and FINTRAC guidelines. It applies to all employees, agents, and operations of ARTCLUB 88 FINANCE CORPORATION.

1.2. As an MSB registered with FINTRAC, we are required to implement a compliance program that includes client identification, record keeping, reporting, and know-your-client processes to prevent misuse of our services for ML/TF.

1.3. Our operations involve virtual currency dealings, triggering additional obligations such as the travel rule for VC transfers.

2. Compliance Officer

2.1. We appoint a Compliance Officer responsible for the implementation and oversight of the AML/CFT program. The officer has direct access to senior management and sufficient authority to enforce compliance.

2.2. The Compliance Officer ensures policies are updated, conducts risk assessments, oversees training, and manages reporting to FINTRAC.

3. Policies and Procedures

3.1. Our written policies and procedures are kept current, approved by senior management, and accessible to all relevant personnel. They cover:

- Client identification and verification methods.
- Establishing and monitoring business relationships.
- Ongoing transaction monitoring for suspicious activities.
- Record keeping requirements.
- Reporting thresholds for large cash/virtual currency transactions (\$10,000 CAD+), EFTs, and STRs.
- Travel rule for EFTs and VC transfers (requiring originator/beneficiary information; risk-based decisions to suspend/reject incomplete transfers).
- Enhanced measures for high-risk clients/situations (e.g., PEPs, high-risk jurisdictions).
- Sanctions screening against Canadian and international lists.

3.2. Procedures include steps for when obligations are triggered, required information, timelines, and reasonable measures to take if information is unavailable.

4. Risk Assessment

4.1. We conduct and document a risk assessment evaluating ML/TF/sanctions risks based on:

- Clients and business relationships (e.g., PEPs, high-volume traders).
- Products, services, and delivery channels (e.g., virtual currency P2P exchanges, online platforms).
- Geographic locations (e.g., transactions involving high-risk jurisdictions per FATF).
- New technologies (e.g., blockchain, wallets).
- Affiliates and other factors (e.g., employee risks).

4.2. Risks are categorized as low, medium, or high. High-risk scenarios require enhanced due diligence, such as verifying source of funds/wealth, increased monitoring, or senior approval.

4.3. The assessment is updated at least every two years or when business changes occur.

5. Client Identification and Verification

5.1. We identify and verify clients before establishing a business relationship or conducting transactions requiring verification (e.g., EFTs/VC transfers \$1,000 CAD+, large cash/VC \$10,000 CAD+)

5.2. Methods of Verification:

- **Government-Issued ID:** Dual process (e.g., credit file + bank statement) or single process (photo ID with name, photo, ID number).
- **In-Person:** Verify ID matches the person; record details.
- **Non-Face-to-Face:** Use certified methods (e.g., credit bureau check, government database) or rely on agents under agreement.
- For entities: Verify existence (e.g., corporate registry), beneficial owners (25%+ ownership), and control structure.

5.3. For PEPs/HIOs: Determine status, obtain senior approval, verify source of funds/wealth, and apply enhanced monitoring.

5.4. We do not proceed if verification fails or suspicions arise.

6. Ongoing Monitoring and Record Keeping

6.1. We monitor business relationships for consistency with client profiles and detect anomalies.

6.2. Records include:

- Client ID documents (retained 5 years post-relationship end).
- Transaction details (e.g., amount, parties, purpose; 5 years post-transaction).
- Reports submitted to FINTRAC (copies retained 5 years).

6.3. For VC transfers: Retain travel rule information.

7. Reporting

7.1. Submit to FINTRAC:

- STRs within 30 days of suspicion.
- Large cash/VC reports (\$10,000 CAD+).
- EFT/VC transfer reports (\$10,000 CAD+ international).
- Terrorist property reports immediately.

7.2. If a transaction poses risk of thwarting ML/TF investigation, we may delay it as per FINTRAC guidance.

8. Training Program

8.1. All employees and agents receive ongoing training on:

- ML/TF methods and indicators.
- PCMLTFA obligations.
- Company policies/procedures.
- Roles in detection/reporting.

8.2. Training is documented, delivered annually or as needed, and tailored to roles (e.g., enhanced for client-facing staff).

9. Two-Year Effectiveness Review

9.1. Every two years, we review the program's effectiveness through internal/external audit, covering all elements.

9.2. Findings are documented, deficiencies corrected, and reported to senior management.

10. Fraud Prevention

10.1. We implement anti-fraud measures integrated with AML/CFT, including transaction monitoring and risk-based assessments.

10.2. Re-verify clients if anomalies arise.

11. Reasons for Refusing or Terminating Relationships

We refuse or terminate if:

- Client refuses verification.
- High-risk indicators (e.g., sanctions list, PEP without mitigation).
- Suspicion of ML/TF.
-

12. Concluding Provisions

12.1. This Policy may be amended unilaterally; clients will be notified via email.

12.2. Available on our website.

12.3. Enters into force on November 11, 2025.

Approved by Senior Management of ARTCLUB 88 FINANCE CORPORATION

Date: November 11, 2025