VANUATU FINANCIAL SERVICES COMMISSION

GUIDELINES ON PROLIFERATION FINANCING FOR VASP

(February 2026)

SUPERVISION DEPARTMENT

Application of Guidelines

Applies to all VASPs and relevant licensees. It should be read together with the Act, the AML framework in Vanuatu, and VFSC/FIU directions.

Virtual Asset Service Providers (VASPs) in Vanuatu, licensed under the Virtual Asset Services Providers Act No. 3 of 2025, must implement robust PF controls to align with FATF Recommendations 1, 7, 12, 15, and their Interpretive Notes, treating PF as an integral part of AML/CFT frameworks. VASPs, including those offering exchanges (Class D), transfers (D1), custody (D2), and other services, face elevated PF risks due to virtual assets', speed, and cross-border nature, often exploited for sanctions evasion by WMD proliferators. These guidelines build on prior Financial Dealers Licensing Act measures, mandating risk-based approaches to prevent funding of weapons of mass destruction programs

1. Objective and Scope

Purpose:
To provide Virtual Asset Service Providers (VASPs) operating in Vanuatu with a risk-based framework to **prevent, detect, and mitigate proliferation financing**, consistent with the FATF Recommendations.

Scope:
This guideline applies to all VASPs licensed or operating in Vanuatu, including but not limited to:

- crypto exchanges,
- custodial wallet providers,
- token issuers,
- decentralized finance (DeFi) platforms acting as intermediaries,
- virtual asset transfer services.

2. Definitions

For the purpose of this guideline:

- **Proliferation Financing (PF):** The financial support, whether direct or indirect, for the development, acquisition, manufacturing, or transfer of

weapons of mass destruction (WMD) and their delivery systems, including financing proliferation-related activities by state or non-state actors.

- **Virtual Assets:** Digital representations of value that can be traded or transferred electronically.
- **Virtual Asset Service Providers (VASPs):** Entities that provide services involving virtual assets including exchange, custody, transfer, or issuance.

3. Regulatory and Legal Framework

VASPs in Vanuatu must comply with:

3.1 AML/CFT Law

- The **Anti-Money Laundering and Counter-Terrorist Financing Act**
- Relevant regulations covering PF compliance and reporting obligations.

3.2 UN and International Sanctions

VASPs must implement controls to block or freeze funds related to individuals and entities designated under:

- **UN Security Council Resolutions** related to WMD/PF sanctions.
- Domestic sanctions lists (as applicable).
- Any other sanctions adopted by Vanuatu relevant to PF.

4. Risk Assessment (PF-Specific)

4.1 Enterprise-Wide PF Risk Assessment

VASPs must conduct an enterprise-wide risk assessment that includes:

- Customer base analysis for PF risk,
- Products/services offered with higher PF exposure (e.g., high-value transfers),
- Delivery channels, including remote onboarding,
- Geographical risk factors,
- Use of technologies that may obscure transactional flows (e.g., mixers, privacy coins).

4.2 Ongoing Review

Risk assessments must be updated when:

- New products/technologies are introduced,
- Regulatory changes occur,
- Indicators of PF emerge.

5. Customer Due Diligence (CDD) & Enhanced Due Diligence (EDD)

Customer Due Diligence (CDD) and VASP-Specific Travel Rule

Apply risk-based CDD, including verifying beneficial owners, source of virtual assets/funds, and wallet screening against UN PF sanctions lists via the Sanctions Secretariat. For transactions over VUV 75,000 or equivalent (~USD 650), comply with FATF Travel Rule (R.16): collect and transmit originator/beneficiary data (name, address, wallet addresses) between VASPs, retaining records for 10 years. Enhanced due diligence for high-risk wallets, such as those interacting with sanctioned addresses or DeFi protocols masking illicit flows

5.1 Standard CDD Requirements

VASPs must collect and verify:

- Identity for individuals,
- Legal existence for entities,
- Beneficial ownership information,
- Purpose and intended nature of the business relationship.

5.2 PF-Focused EDD

Apply EDD when:

- The customer is a politically exposed person (PEP) or state-related entity,
- Transactions involve high-risk jurisdictions or countries with proliferation concerns,

- Transactions involve large values, frequent transfers, or layering patterns.

EDD measures include:

- Enhanced verification of source of funds and wealth,
- Scrutiny of transactional purpose,
- Screening against PF lists.

6. Screening and Sanctions Compliance

6.1 Sanctions and PF Lists

Regularly screen customers and transaction parties against:

- **UN sanctions lists related to PF**,
- National and regional PF sanctions lists,
- FATF issued lists of high-risk jurisdictions.

Screening frequency:

- At onboarding,
- On an ongoing periodic basis,
- Real-time for transactions.

6.2 Blocking and Reporting

When hits arise:

- Immediately **freeze/block** the virtual asset funds,
- Report to the **Financial Intelligence Unit (FIU) of Vanuatu**,
- Do not execute transactions with listed entities.

Records of screenings and actions must be retained.

7. Transaction Monitoring Systems

7.1 Automated Monitoring

VASPs must implement systems capable of:

- Detecting suspicious patterns indicative of PF (e.g., structuring, rapid outbound transfers),
- Flagging transactions involving high-risk jurisdictions,
- Monitoring unusual velocity of virtual asset movements.

7.2 Red Flags for PF

Examples include but are not limited to:

- Transactions from newly created accounts with high amounts,
- Use of intermediary wallets with no clear economic purpose,
- Layered transfers across multiple chains to obscure origin,
- Engagement with IP addresses from high-risk jurisdictions.

8. Reporting Obligations

8.1 Suspicious Transaction Reports (STRs)

VASPs must file STRs to the **Vanuatu FIU** when:

- PF is reasonably suspected,
- Transactions cannot be explained on a legal basis,
- Screening hits remain unresolved.

Reports must be timely, factual, and include all relevant transaction and identification data.

8.2 Threshold Reporting

There is no threshold exemption for PF suspicions — **any value** should be reported if risk indicators are present.

9. Record Keeping

Maintain records for **at least 7 years**:

- Customer documentation,
- CDD and EDD files,
- Transaction logs,

- Screening results and risk assessments,
- STR submissions.

10. Internal Controls and Governance

10.1 Senior Management Responsibility

Senior management must:

- Approve risk management policies,
- Allocate resources to compliance functions,
- Ensure PF oversight.

10.2 Compliance Function

Designate a **Compliance Officer** tasked with:

- Implementing this guideline,
- Reporting to senior management,
- Coordinating with FIU and regulators.

10.3 Independent Audit

Conduct periodic independent reviews of PF controls and remediation.

11. Training and Awareness

Provide targeted training to relevant staff on:

- PF risks and indicators,
- Sanctions requirements and screening tools,
- Reporting procedures.

Training frequency:

- Onboarding,
- Annually,
- Upon major regulatory updates.

12. Use of Technology and Cryptographic Tools

To mitigate PF risk:

- Leverage blockchain analytics tools,
- Use address scoring databases for high-risk assessments,
- Monitor decentralized exchange (DEX) flows where possible.

13. Cooperation with Law Enforcement

VASPs must, where permitted by law:

- Provide information to competent authorities,
- Respond promptly to lawful information requests,
- Support investigations into PF.

14. International Cooperation and Correspondent VASP Relationships

When interacting with foreign VASPs:

- Assess their PF compliance regimes,
- Include contractual clauses requiring adherence to international standards,
- Exchange information on suspect accounts subject to data protection regimes.

15. Enforcement and Penalties

VASPs that fail to comply with PF obligations may be subject to:

- Regulatory sanctions,
- License revocation,
- Fines and penalties under Vanuatu law.

Please contact the following person should you have any questions:

Mr. Joshua Tari
Manager, Supervision Department
Email: tjoshua@vfsc.vu
Phone: (678) 22247
Fax: (678) 22242

Dated this 17th day of February 2026

Branan Karae

Commissioner