Understanding Financing of Proliferation of Weapons of Mass Destruction

Banco de Moçambique (BM)
Prudential Supervision Department (DSP),
Anti-Money Laundering and Countering the Financing of Terrorism (SBF) Service

Contents

Introduction

The Banco de Moçambique (BM), as the regulator of credit institutions, financial companies and the Mozambique Stock Exchange, shall ensure compliance with the legislation on anti-money laundering, countering the financing of terrorism and proliferation of weapons of mass destruction by the obliged institutions.

Thus, this material aims to improve the understanding by entities, institutions, and individuals on proliferation financing matters, in order to ensure knowledge of the consequences of non-compliance with legal obligations and knowledge of some red flags of sanctions evasion as a way to prevent supervised institutions from being misused for financing of proliferation (FP).

Acronyms

CFP – Countering the Financing of Proliferation

DNFBPs - Designated Non-Financial Businesses and Professions

DPRK - Democratic People's Republic of Korea

FATF - Financial Action Task Force

FP – Financing of Proliferation

KYCC – Know Your Customer's Customer

ML/FTP – Money Laundering/Financing of Terrorism and Proliferation

MVTS – Money or Value Transfer Services

UN – United Nations

UNSC – United Nations Security Council

UNSCR – United Nations Security Council resolution

WMD - Weapons of Mass Destruction

Goals

- Define financing of proliferation and present a few delivery systems;
- Present the internal consequences of financing of proliferation;
- Identify red flags of sanctions evasion;
- Present the consequences of non-compliance with legal obligations and international best practices;
- Present UN obligations and FATF standards;
- Identify sectors vulnerable to exploitation of proliferation financing.

Definitions of Financing of Proliferation of Weapons of Mass Destruction

Financing of Proliferation (FP)

According to FATF, it consists of providing funds or services that can be used, in whole or in part, for the creation of weapons of mass destruction (WMD).

In accordance with the resolutions of the United Nations Security Council (UNSCR) – Financing of proliferation is defined through resolutions 1540, 1718, and 2231.

Applicable Legislation

- **Law No. 14/2013, of August 12 -** Anti-Money Laundering and Counter-Terrorism Financing Act;
- **Law No. 15/2023, of August 28** - Anti-Money Laundering, Countering and Suppressing Terrorism and Proliferation of Weapons of Mass Destruction
- **Decree No. 53/2023 of August 31 –** Approves the regulation of Law No. 14/2023 of August 28;
- **Decree No. 54/2023, of August 31 –** Approves the Regulation of Law No. 15/2023 of August 28;
- **Notice No. 5/GBM/2022, of November 17 –** Approves the Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Guidelines.

Internal Consequences of Proliferation Financing

Main Consequences

- Reputational damage;
- Increase in crime and illicit activities;
- Potential loss of revenue;
- Secondary sanctions.

What do proliferators want?

- **Money –** purchase necessary components for WMDs, supply illicit networks abroad and support national leadership.
- **Goods –** Create WMD - dual-use goods, raise funds for the creation of WMD and support national leadership.

Common Methods of Sanctions Evasion by the DPRK

Some fundraising tactics for arms programs:

- Arms trafficking and military support;
- Work abroad;
- Ship records;
- Ship identity falsification;
- Ship-to-ship transfers;
- Use of diplomatic immunity.

Identifying warning signs of sanctions evasion

Indicators of shell or ghost companies

- Lack of online presence;
- No physical location;
- No address or phone number;
- Sharing information with a sanctioned entity.

Maritime indicators

- Ship-to-ship transfers in suspicious locations;
- Staying in suspicious places;
- Owned or operated by shell companies;
- No AIS (Automatic Identification System) transmission signal in suspicious locations;
- Registered in a high-risk jurisdiction.

Transport and transaction indicators

- Nonsensical shipping route from a financial standpoint;
- The final destination is a forwarder;
- Lack of sales information or mention of a country that raises proliferation concerns;
- The shipment passes through a country with diversion concerns.

UN obligations and FATF standards

The UN mission, which includes peacekeeping and Chapter VII of the UN Charter, gives the Security Council (UNSC) authority to issue binding resolutions to Member States.

Financing or other support for AMD programs is illegal under international law.

The UNSC's counter-proliferation obligations form the basis of counter-proliferation financing activities worldwide.

UNSC resolutions

UNSC Resolution 1540

- Responds to terrorism and WMD proliferation concerns;
- Implications for state-funded and non-state-funded programs;
- Imposes duties to prevent the proliferation of nuclear, chemical or biological weapons and their means of delivery;
- Introduced legal requirements to counter the financing of proliferation.

UNSC Resolution 1718 (2006): North Korea

- Creation of the Sanctions Committee to inspect relevant sanctions concerning relevant sanctions concerning the DPRK;
- Publication of semi-annual reports on investigations associated with DPRK sanctions and incidents of non-compliance;
- Publishes names of specific persons, entities, and activities associated with financing or material support for DPRK WMD programs.

UNSC Resolution 2231(2015): Iran

- Discourages the development of ballistic missiles in Iran; existing sanctions apply mainly to individuals and entities associated with ballistic missile activity.

FATF and Countering Proliferation Financing

Recommendation 1: Proliferation financing risk assessments
(Art. 57, Law 14/2023 of August 28)

- Adds “risk of financing of proliferation” to the current recommendation.

Recommendation 2: National coordination and cooperation
(Art. 65, Law 14/2023 of August 28)

- Includes counter-proliferation financing obligations, under UNSCR 1540.

Recommendation 7: Specific financial sanctions related to proliferation
(Art. 10, Law 14/2023 of August 28)

- Scope limited to specific financial sanctions on the DPRK and Iran under the UNSCR.

Immediate outcome 11: Financial sanctions against proliferation

- Persons and entities involved in WMD proliferation are prohibited from raising, moving and using funds in accordance with relevant UNSC resolutions.

Consequences of Non-Compliance with International Best Practices Obligations

UN

- Non-compliance with UN resolutions causes the potential for:
  - Reputational damage;
  - Reduced cooperation with other countries on a range of diplomatic issues;
  - Unilateral primary sanctions of individual countries;
  - Unilateral secondary sanctions of individual countries;
  - UN sanctions.

FATF

- Non-compliance with FATF resolutions provide for potential:
  - Reputational damage
  - Placement on the FATF list of countries requiring additional monitoring (the FATF “grey list”);
  - Less external investment;
  - Reduction of citizens' access to global financial markets;

FATF Best Practices Guide

The Financial Action Task Force's 2018 Best Practices Guide on Countering the Proliferation of Financing (CFP) highlights:

- CFP obligations for governments and the private sector;
- Best practices for implementing CFP sanctions.

Identifying proliferation financing vulnerabilities

Domestic vulnerabilities

- Legal, institutional or regulatory context;
- Handling of legal persons and provisions;
- Economic and technological factors;
- Political and social factors;
- Geographical and environmental.

Sectoral vulnerabilities

- Financial system;
- Designated Non-Financial Businesses and Professions (DNFBPs):
- Trade-related sectors.

Financial Sector Vulnerabilities

Financial institutions

- Vulnerable to FP through the rendering of financial services to individuals or entities that have been subject to financial sanctions;
- Areas of vulnerability include banking correspondence relationships, making it more important to know your customer's customer (KYCC);
- Enhanced monitoring of activities related to North Korea (DPRK) embassies.

Money or Value Transfer Services (MVTS)

- The various services, providers and customers mean that MVTS can be challenging to regulate;
- They can operate in limited corridors, often to serve diaspora communities;
- The international transfers and the currency exchange shall be supervised based on risk.

Financial Sector Vulnerabilities (Cont'd.)

Financial Technologies

Information technology security is currently even greater in the financial sector, not only for the monetary amounts involved, but also for the sensitive and private information of customers and organizations. Financial technologies involve mobile payment systems, digital marketplaces and challenger banks.

- **Mobile payment systems**

  Examples: Square, Apple Pay, Venmo, Google Pay, PayPal.

- **Digital markets**

  Examples: Alibaba, Amazon Pay, eBay.

- **Challenger banks (neo-banks)**

  Examples: Revolut, N26, Starling, Monzo.

DNFBP vulnerabilities

Proliferators may turn to professional service providers for the purpose of proliferation financing due to their nature (acting on behalf of a third party and moving high sums of money).

- Accountants;
- Lawyers;
- Notaries;
- Gem and precious metal traders;
- Car dealers;
- Realtors;
- Casino managers;
- Fund managers.

Vulnerabilities of trade-related sectors

Maritime industry: business structures that facilitate the evasion of maritime sanctions.

Global maritime shipping is highly complex and involves many entities from around the world:

- Shipping insurers;
- Ship brokers;
- Ship managers, carriers, and supply operators

Front or shell companies may disguise the beneficial/ultimate owner or end user of the goods and services.

Vulnerabilities of trade-related sectors (Cont'd)

- Large volumes of trade put the ports in high risk of transshipment;
- Insurance can be difficult to enforce independently, allowing ships used for proliferation to obtain it despite bans:
    - UNSCR 2321 *All Member states are prohibited from providing classification, certification or related services, as well as insurance or reinsurance, to vessels flying the flag of the DPRK, whether owned, controlled or operated by them.*

FATF guidelines: how to avoid sanctions violations

- Consider the complex products or services, distributed across borders, easily accessible and involving a number of customers can be easily exploited;
- Consider the following points in transactions to detect proliferation warning signs:
  - What is the frequency of transactions and the amounts concerned?
  - Does the client appear to be working for shell or ghost companies?
  - Who is the ultimate beneficiary of the transaction? (for example, a purchase made for someone who is in an unrelated business)
  - Does the good or service pass through a high-risk jurisdiction?

Best anti-proliferation financing practices for the financial sector

- Screening all customers, including ultimate beneficiaries, legal entities, prior to entering into a business relationship;
- Applying appropriate due diligence measures for each type of customer;
- Have systems capable of detecting complex and uncommon patterns
  or suspicious transactions;
- Increased monitoring of transactions to and from countries considered tax havens and / or sanctioned;
- In case of suspicion, immediately block
  funds and report to the competent bodies;
- Act in compliance with the legal instruments concerned.

Sources

- https://pt.wikipedia.org/wiki/Conselho_de_Seguran%C3%A7a_das_Na%C3%A7%C3%B5es_Unidas
- https://www.un.org/securitycouncil/
- https://data.europa.eu/data/datasets/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions?locale=pt
- https://portalbcft.pt/pt-pt/content/recomenda%C3%A7%C3%B5es
- https://www.io.gov.mo/pt/legis/int/rec/658
- https://www.io.gov.mo/pt/legis/int/rec/1787
- Chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.vertic.org/media/assets/nim_docs/NIM%20Tools%20(Factsheets)/FS6_UNSCR_PT_MAY_2011.pdf

THANK YOU!