



REPUBLIC OF ZAMBIA

GOVERNMENT GAZETTE

Published by Authority

Price: K35.00 net
Annual Subscription: K650.00

No. 7708]

Lusaka, Friday, 31st January, 2025

[Vol. LXI, No.12

GAZETTE NOTICE No. 87 of 2025

[1144727

Anti-Terrorism and Non-Proliferation Act
(No. 6 of 2018)

National Anti-Terrorism Centre Guidelines on the Implementation of Targeted Financial Sanctions on Terrorism and Proliferation Financing

These Guidelines are authored by the National Anti-Terrorism Centre (NATC) in line with the Anti-Terrorism and Non-Proliferation Act No. 6 of 2018 as amended and the Anti-Terrorism and Non-Proliferation (Implementation of United Nations Security Council Resolutions) Regulations, 2024 ("Statutory Instrument No. 1 of 2024.") of the Republic of Zambia for comprehensive use by reporting entities, supervisory authorities, State institutions and any other person or entity. The guidelines are indicative and while due care was exercised to ensure that these guidelines are accurate and consistent with the Anti-Terrorism and Non-Proliferation Act No. 6 of 2018 as amended, the latter shall prevail in the unfortunate case of ambiguity.

LUSAKA

J. KAMVUMA,
Director-General

ACRONYMS

AML	Anti-Money Laundering
AML	Anti-Money Laundering
BO	Beneficial Owner
CDD	Customer Due Diligence
CFT	Countering The Financing Of Terrorism
CPF	Countering Proliferation Financing
DNFBPS	Designated Non-Financial Businesses And Professions
DPRK	Democratic People's Republic of Korea
FATF	Financial Action Task Force
FSPS	Financial Service Providers
FI	Financial Institution
FIC	Financial Intelligence Centre
ML	Money Laundering
NATC	National Anti-Terrorism Centre
PF	Proliferation Financing
PRR	Positive Return Report
RBA	Risk Based Approach
STR	Suspicious Transaction Report
TF	Terrorism Financing
TFS	Targeted Financial Sanctions
UN	United Nations
UNSCR	United Nations Security Council Resolutions
VAS	Virtual Assets
VASPS	Virtual Asset Service Providers
WMD	Weapons of Mass Destruction

1.0 Introduction

These Guidelines are issued by the National Anti-Terrorism Centre (Hereinafter referred to as 'The Centre') Pursuant to the Requirements in the United Nations Security Council Resolutions (Unscrs) for State Parties to take and enforce effective measures to prevent the financing of both Terrorism and Proliferation. In conformity with the Unscrs and Financial Action Task Force (Fatf) recommendations, Zambia enacted the Anti-Terrorism and Non-Proliferation Act No. 6 of 2018 and issued regulations for the implementation of Targeted Financial Sanctions (Tfs) related to Terrorism Financing (Tf) and Proliferation Financing (Pf). The guidelines are issued to assist or Entity in the implementation of Tfs and are hereby released to enhance compliance.

In particular, the guidelines provide guidance to reporting entities, Supervisory Authorities, State Institutions and any other person or entity, or a Virtual Asset Service provider that might be holding funds or other Assets of a nationally listed person, Group or Entity or a designated person or entity on how Tfs should be implemented in Zambia.

2.0 Objectives

The objectives of these guidelines are to:

- (a) Assist reporting entities, Supervisory Authorities, State Institutions and any other person in complying with the requirements of the Law and regulations relating to Tf and Pf;
- (b) Provide guidance to reporting entities, Supervisory Authorities, State Institutions and any other person on implementing (TFs) prevent and suppress TF and PF in accordance with the relevant Unscrs;
- (c) Enable the Natc and other Competent Authorities (Ca) monitor compliance with Tfs Measures related to Tf and Pf by reporting entities, Supervisory Authorities, State Institutions and any other person; and
- (d) Raise awareness of Tf and Pf risks.

3.0 Domestic AML/CFTP Framework

These Guidelines should be read within the Framework of:

- (a) Anti-Terrorism and Non-Proliferation Act No. 6 of 2018 (As Amended) and its Regulation, 2024;
- (b) Financial Intelligence Centre Act No. 46 Of 2010 (as amended);
- (c) Prohibition and Prevention of Money Laundering Act No. 14 Of 2001, (as amended);
- (d) Ionising Radiation Protection Act, No 16 of 2005;
- (e) Cyber Security and Cyber Crimes Act No. 2 of 2021
- (f) Mines And Minerals Development Act No. 11 of 2015
- (g) Forfeiture of Proceeds of Crime Act No. 19 of 2010;
- (h) The Public Interest Disclosure Act No. 4 of 2010;
- (i) Immigration and Deportation Act No. 18 of 2010
- (j) The Anti-Corruption Act, No. 3 of 2012;
- (k) Mutual Legal Assistance in Criminal matters Act Chapter 98 of the Laws of Zambia;
- (l) The Non-Governmental Organisations Act, No. 16 of 2009; And
- (m) The Penal Code Act, Chapter 87 of the Laws of Zambia.

4.0 International AML/CFT Framework

The table below summarizes the distinguishing components of the various UNSCRS and FATF requirements:

UNSC Resolution	UNSCRS List	FATF Requirements	National List
	UNSCR 1267 (1999)/ 1989 (2011) And 2253 (2015) Concerning ISIL (Da'esh) Al- Qaida and Associated Individuals Groups Undertakings and Entities and other subsequent resolutions (ISIL (Da'esh) Al-Qaida List).	-Recommendation 6 (Targeted Financial sections related to terrorism and terrorist financing)	UNSCR 1373(2001)
	UNSCR 1988 (2011) Concerning the Taliban and the Subsequent Resolutions (Taliban List).	-Immediate Outcome 9 ¹ - Immediate Outcome 10 ²	
	UNSCR 1540 (2004) Concerning Proliferation of Weapons of mass destruction (DPRK) UNSCR 1718 (2006) and Islamic Republic of Iran UNSCR 2231(2015)	-Recommendation 7 (Targeted financial sections related to Proliferation) -Immediate Outcome 11 ³	

Note 1:

The Sanctions Committee in relation to terrorism was initially established pursuant to Resolution 1267 (1999), which imposed a limited air embargo and assets freeze on the Taliban. Over time, the regime evolved and the measures were expanded to include targeted assets freeze, travel ban and arms embargo against designated individuals and entities. On 17th June, 2011, the Security Council unanimously adopted Resolutions 1988 (2011) and 1989 (2011). With the adoption of these resolutions, the Security Council decided that the list of individuals and entities subject to the measures would be split in two. The Committee was henceforth known as the Al-Qaida Sanctions Committee, mandated to oversee implementation of the measures against individuals and entities associated with Al-Qaida. A separate Committee was established pursuant to resolution 1988 (2011) to oversee implementation of the measures against individuals and entities associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan. On 17th December, 2015, the Security Council unanimously adopted resolution 2253 (2015). With the adoption of this resolution, the Security Council decided to expand the listing criteria to include individuals and entities supporting the Islamic State in Iraq and the Levant (ISIL).

Note 2:

On April 28, 2004, the UN Security Council unanimously voted to adopt Resolution 1540, a measure aimed at preventing non-state actors from acquiring nuclear, biological, and chemical weapons, their means of delivery, and related materials. The resolution filled a gap in international law by addressing the risk that terrorists might obtain, proliferate, or use weapons of mass destruction. Adopted under Chapter VII of the UN Charter, UNSCR 1540 formally establishes the proliferation and possession of WMD by non-state actors as “a threat to international peace and security.” The resolution mirrors the approach taken under UNSCR 1373 in 2001, which required all countries to adopt national counter-terrorism laws, and imposes legally binding obligations on all states to adopt “appropriate effective” measures to prevent the proliferation of WMD to non-state actors.

5.0 Freezing of Funds or Other Assets**5.1 Accessing The Lists****Subject To Regulation 21**

- (a) The Consolidated United Nations Sanctions list and the National list can be accessed from the Un Website <https://www.un.org/securitycouncil/Content/un-sc-consolidated-list> (UN list only) and the NATC website www.natc.gov.zm
- (b) Both The UN And National List are updated periodically by adding, deleting and amending.
- (c) Subscribe to the NATC mailing list to receive updates.
- (d) Upon receipt of the list from the UN, the Centre disseminates to all reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider within 7 hours. Reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider will scan their databases and implement Targeted Financial Sanctions within 16 hours.
- (e) All reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider who access the UN consolidated sanctions list in accordance with (a) above will scan their databases and implement Targeted Financial Sanctions within 16 hours and furnish a report to the Centre in accordance with Regulation 9.

5.2 Screening

- (a) Subject to regulation 8 and 10, reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider are required to carry out regular and ongoing screening against updated UN Sanctions Lists and the national list prior to conducting any transaction or undertaking any financial services to ascertain whether the name of such a person or entity is on the lists. Specifically, screening should be conducted during the following:
 - (i) On-boarding a new customer;
 - (ii) Facilitating an occasional transaction (including domestic and international wire transfers);
 - (iii) Establishing any relationship with any person or entity;
 - (iv) Upon updates on the National List and UN Sanctions List; and
 - (v) Upon review of Know-Your-Customer/Client (KYC) or changes to a customer's/client's information
- (b) Screening and implementation of TFS must be conducted within 16 hours to ensure compliance with the requirement for implementing freezing measures without delay and without prior notice (the subject must never be Made Aware).
- (c) Reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider are required to screen their entire customer/client database daily and whenever an update has been made to the UN Sanctions List or National List, to prevent the dissipation of funds of the designated persons or entities. The Centre maintains the UN and National Lists and on a daily basis, monitor the United Nations Sanctions Lists for any updates.
- (d) Reporting entities, supervisory authorities, State Institutions and any other person or entity, or a virtual asset service provider must establish and implement screening and transaction monitoring systems and are encouraged to also monitor the UN Sanctions List.

- (e) Screening should be undertaken for existing customers, potential customers, beneficial owners, and transactions to identify possible positive matches.

(i) Positive Match

A positive match is when a designated persons or entities, or Nationally Listed person, group or entity matches all the key identifiers published on the Sanctions Lists. The range of information that constitute identifiers of are as follows:

(1) For Natural Person:

- (a) Name
- (b) Aliases/also known as/formerly known as
- (c) Date of birth
- (d) Nationality
- (e) National Identification Card or Passport or Refugee Identification Card
- (f) Last known physical address
- (g) Or any other identifying information available other relevant information

(2) For groups or entities:

- (a) Name(S)
- (b) Aliases also known as/formerly known as
- (c) Certificate of incorporation
- (d) Registered address
- (e) Address of branches
- (f) Other information

- (f) Where the person, group, or entity matches all the key identifiers published on the Sanctions Lists, the result is considered A 'Positive Match'. Where the positive match is an existing customer/client, reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider are required to, identify and freeze, without delay and without prior notice, all funds or other assets owned or controlled by the designated person or entity or Nationally Listed person, group or entity in their possession.
- (g) Where the positive match is a potential customer/client, the reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider are required to reject the transaction without delay and report to the NATC and FIC. However, before rejecting the transaction, reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider are required to search their records to confirm whether the potential customer/client is a Beneficial Owner (BO).
- (h) Where the search is positive, reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider are required to identify and freeze, without delay and without prior notice, all funds or other assets owned or controlled by the BO in their possession.
- (i) In cases of positive matches (for either existing or potential customer/client), reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider are required to report to the NATC, without delay, any funds or other assets frozen or actions taken in compliance with the prohibition requirements of the relevant UNSCRs including attempted transactions.
- (j) In addition, reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider are required to without delay file a positive return report to the NATC and, for reporting entities, a Suspicious Transaction Report (STR) to the FIC.

(ii) False Positive

- (1) A false positive is a potential match to designated person or entities or Nationally Listed person, groups or entities either due to similarity in names, ambiguous identifying data or wrong entries on the Sanctions List, which, on evaluation, proves not to be a positive match.
- (2) Reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider are required to obtain additional information and identification documents from the customer/client or a third party to ascertain whether a customer/client is a designated person or entity or nationally listed person, group or entity in the case of similar names.
- (3) Reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider are required to forward an inquiry to the Centre to ascertain whether the customer/client is a designated person or entity or nationally listed person, group or entity in the case of similar names. Any inquiry submitted to the Centre is to be accompanied by additional information, copies of identification documents and the reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider's assessments.

- (4) Where reporting entities, supervisory authorities, State institutions and any other person or entity, or a Virtual asset service provider receive feedback from the Centre that the customer/client, potential customer/Client Or BO is not the designated person or entity or nationally listed person, group or entity, they should unfreeze the funds or other assets without delay. Where the customers/clients discover that their accounts have been mistakenly frozen or transactions have been mistakenly rejected or blocked, the reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider shall advise their customers/clients to contact the Centre to verify the false positive match. The contact details for the Centre in relation to TFS on TF And PF is: info@NATC.gov.zm

(iii) Attempted Transaction

An Attempted Transaction could be classified as one that a customer/client intended to conduct with a reporting entity, supervisory authority, State institution and any other person or entity, or a virtual asset service provider and took some form of action or activity to do so. An Attempted Transaction is different from a single request for information, such as an enquiry about the fee applicable to a specific transaction. The customer/client must enter into negotiations or discussions with the reporting entity, supervisory authority, State institution and any other person or entity, or a virtual asset service provider to conduct the transaction or activity and such activity must involve a tangible act to be taken by either the customer/client or the reporting entity, supervisory authority, State institution and any other person or entity, or a virtual asset service provider. A reporting entity, supervisory authority, State institution and any other person or entity, or a virtual asset service provider is required to report attempted transactions by a designated person or entity or nationally listed person, group or entity or related parties to the NATC where there is no existing business relationship with the customer/client and no such business relationship is subsequently established. This may include any transaction that is subsequently rejected or blocked, incomplete in the event of failure to satisfactorily complete CDD and attempt for redemption of funds or other assets where repayment has been made.

(iv) Potential Match

A potential match is when there is a partial match between identifiers in the Sanctions Lists with any information in the database held by reporting entities, supervisory authorities, State institutions and any other person or entity, including a virtual asset service provider, and the reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider are unable to conclude a false positive or a positive match. Due to prevalence of some names, FIs may find various potential matches. However, it does not necessarily mean that the individual, entity, or group they are dealing with is subject to TFS. Reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider are required to cross-check their customers' database with the identifiers published on the Sanctions Lists when identifying the potential match, by taking into consideration their knowledge of the customer/client, potential customer/client and BO or transaction, through CDD and/or other sources of information. Where reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider are unable to internally verify whether the 'potential match' is a false positive result or a confirmed match, the transaction should be suspended, and the case reported to NATC. The reported transaction should remain suspended, until a response is received on the status of the potential match.

5.3 Screening of Customers – Related and Third Parties

- (a) reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider are required to undertake further screening and analysis of designated persons or entities whose properties or accounts are jointly owned and/or indirectly controlled by the designated persons or entities.
- (b) reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider are required to conduct further Customer Due Diligence (CDD) on parties related to frozen accounts including checking on the control and conduct of the frozen accounts and other related or third parties accounts connected to designated persons or entities.
- (c) The requirements for CDD on legal persons and legal arrangements and beneficial owners in the respective provisions under the Centre Act and Regulations should be applied in determining whether the funds or other assets are directly or indirectly owned or controlled.
- (d) reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider are required to screen the names of beneficiaries of wire transfers and assess whether such transactions should be blocked or rejected.
- (e) reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider are also required to search, examine and analyse past financial activities of designated persons or entities and related or third parties.

5.4 Application of Targeted Financial Sanctions

- (a) Following the screening, reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider are required to implement TFS by identifying and freezing, without delay and without prior notice, all funds or other assets owned or controlled wholly or jointly, directly, or indirectly, by the designated person or entity or nationally listed person, group or entity in their possession.
- (b) Reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider are prohibited from providing funds or other assets or rendering financial services or other related services, whether in whole or in part, directly or indirectly, for the benefit of any designated person or entity or nationally listed person, group or entity. Prohibitions include any transfer, conversion, disposition, alteration, use, dealing of funds or other assets which results in changing in their volume, amount, location, ownership, possession, nature or destination or that would in any way enable the use of such funds or other assets for any purpose.
- (c) Reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider shall advise the customer/client or related party of the frozen accounts, blocked or rejected transactions to submit any query or appeal for variation to the frozen accounts, delisting or any other matters to the Centre for approval subject to Section 52 of the ATPNA and Regulation 17.
- (d) TFS in accordance with Regulations 8 and 10, must be implemented if a positive match with the Sanctions Lists is identified.
- (e) No criminal or civil proceedings shall be instituted against a reporting entity, supervisory authority, State institution and any person or implementing these obligations in good faith.

Summary

Register	-Subscribe directly on the UN website to receive sanctions lists -On daily basis check the Centre's website for updated national list
Screening	Screen daily their customers/clients, potential customers/clients, beneficial owners and transactions to identify possible matches
Implement TFS	Freeze and Prohibit funds, Report action taken
Internal Controls	Internal policies procedures to comply with TFS legislation

6.0 Third Party Claims

- (a) A reporting entity, supervisory authority, State institutions and any other person or entity should ensure that once it carries out a freezing action, it takes measures to ensure the reasonable preservation of those funds or other assets so that if there is a successful claim by a bona fide third party, the funds or other assets remain available for the purposes of the third-party claim.
- (b) A claim by a third party does not require a reporting entity, supervisory authority, State institutions and any other person or entity to unfreeze any funds or other assets which are the subject of the claim until a favorable decision is made by the Minister or the matter is disposed of and an appropriate order is duly issued by the court.
- (c) Where a reporting entity, supervisory authority, State institutions and any other person or entity receives a de-listing request in relation to a person, group or entity relating to funds or other assets that are the subject of a third party claim, the funds or other assets should remain frozen until the de-listing request and the third party claim have been finally determined.

7.0 Unfreezing Of Funds Or Other Assets

- (a) Upon receipt of a de-listing notice from the Centre, a reporting entity, supervisory authority, State institution and any other person or entity, or a virtual asset service provider shall, without delay, unfreeze funds or other assets of a formerly designated person or entity or nationally listed person, group, or entity.
- (b) Upon implementing unfreezing measures, a reporting entity, supervisory authority, State institution and any other person shall report to the Centre on action taken without delay from the receipt of delisting notice and include the time and date of unfreezing and a list of the unfrozen funds or other assets
- (c) On the instruction of the Centre, a reporting entity, supervisory authority, State institution and any other person shall unfreeze funds or other assets for certain purposes, including, for example, to reflect the rights of third parties or to implement court orders.
- (d) The person or entity affected is not a designated person or entity and as such was inadvertently affected by the freezing mechanism (i.e. a false positive).
- (e) A reporting entity, supervisory authority, State institution and any other person must continue to monitor updates to the National list so that they are aware that a person, group or entity has been de-listed. Unfreezing should take place without delay but with appropriate due diligence and deliberate caution, consistent with the terms of de-listing and any guidance from authorities.

- (f) Reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider must continue to be vigilant to ensure that accounts or funds or others assets are not transferred to other sanctioned persons, groups or entities. Reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider that have questions about unfreezing the assets of a person, group or entity that has been delisted should seek guidance from the NATC.
- (g) Authorising access to frozen funds or other assets will only be allowed if exemption conditions set out in UNSCRs 1452, 1718 and 2231 or any future successor resolutions have been met.

8.0 *Listing*

8.1 National List

The National List contains full particulars of persons, groups and entities that have been identified and listed at the recommendation of the NATC. The persons, groups or entities on the national list are included when they are reasonably believed or suspected to be involved in the commission, preparation or instigation of acts of terrorism, terrorism financing, proliferation and proliferation financing and are subject to TFS in line with UNSCR 1373, UNSCR 1540 and subsequent resolutions. The national list shall take effect upon circulation by the Centre.

8.2 United Nations Sanctions List

- (a) The United Nations (UN) Sanctions List includes all individuals and entities subject to targeted TFS imposed by the Security Council. The UN Sanctions List includes any individual or entity acting on behalf of or acting at the direction of designated persons or entities or providing support for terrorism, terrorism financing, proliferation, and proliferation financing.
- (b) The UN Sanctions List takes effect upon designation by the relevant Committee.
- (c) The Minister shall identify targets for designation (proposal) based on the designation criteria set out in the relevant United Nations Security Council resolutions (UNSCRs).

9.0 *De-Listing*

9.1 National List

The de-listing of nationally listed persons, groups or entities from the National List shall take effect upon publication through electronic mail, gazette notice, a daily newspaper of general circulation or such media as the Centre may consider appropriate.

9.2 United Nations Sanctions List

- (a) The de-listing of any specified individuals or entities under the United Nations Sanctions List shall automatically take effect when the specified individuals or entities are removed by the relevant sanctions committees.
- (b) The Minister shall follow procedures adopted by the relevant UN sanctions Committee when submitting de-listing requests in the case of persons and entities designated pursuant to the UN Sanctions Regimes.
- (c) With regard to designations pursuant to UNSCR 1988, designated persons or entities may opt to petition Focal Point Person in accordance with Annex 4 for the delisting procedures as stipulated in UNSCR 1730 (2006).
- (d) With respect to designations on the Al-Qaida Sanctions List, procedures for informing designated persons and entities of the availability of the United Nations Office of the Ombudsperson, pursuant to UNSCRs 1904 (2009), 1989 (2011), 2083 (2012), 2161 (2014), 2253 (2015), 2368 (2017), 2610 (2021) and 2734 (2024) to accept de-listing petitions (Refer to Annex 5).
- (e) The Minister shall follow procedures to de-list and unfreeze the funds or other assets of persons and entities which do not, or no longer, meet the criteria for designation. The procedures of the 1267/1989 Committee are set out in UNSCRs 1730; 1735; 1822; 1904; 1989; 2083 and any successor resolutions while the procedures of the 1988 Committee are set out in UNSCRs 1730; 1735; 1822; 1904; 1988; 2082; and any successor resolutions.

9.3 Obligation

Reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider shall implement TFS without delay and without prior notice unless directed otherwise by the Centre subject to Regulations 15, 17 and 18.

10.0 *Obligations*

- (a) In addition to the above, reporting entities, supervisory authorities, State institutions and any other person or entity, or a virtual asset service provider are required to fulfill the following obligations:
 - (i) implement TFS without delay and without notice upon publication of the UN Sanctions List and circulation of the National List;
 - (ii) Cooperate with the Centre in verifying the accuracy of the submitted information;
 - (iii) Implement the freezing, unfreezing¹, and access to frozen funds or other assets when appropriate, without delay;

- (iv) Cooperate with competent authorities to provide information on TFS timeously when required;
- (v) Set and implement policies, procedures, and internal controls to support implementation of TFS;
- (vi) Conduct ongoing TFS training and awareness sessions;
- (vii) Prohibit staff from, directly or indirectly, informing the customer/client or any third party that freezing actions or any other measures will be implemented.
- (viii) Ensure adequate resources are allocated to meet the obligations of implementing TFS.
- (ix) Monitor accounts and transactions against the UN Sanctions List and National List.
- (x) Designate focal point persons for the purpose of implementing TFS who will regularly contact the NATC.

11.0 Sanctions For Non-Compliance With Tfs Obligations

The sanctions contained in Section 72A of the Anti-Terrorism and Non-Proliferation (Amendment) Act, 2024, any other relevant Law or Regulations shall be imposed by the NATC on any reporting entity, supervisory authority, State institution and any other person or entity, or a virtual asset service provider under its regulatory purview that fails to comply with the provision of the reporting requirements.

12.0 Proliferation Financing

The Anti-Terrorism and Non-Proliferation Act No. 30 of 2024 defines Proliferation and Proliferation Financing as follows: *Proliferation means—*

- (a) intentionally and without lawful authority, altering, manufacturing, producing, possessing, acquiring, stockpiling, storing, developing, brokering, transporting, selling, supplying, transferring, exporting, transiting, transshipping, disposing, or dispersing or using of a chemical, biological, radiological or nuclear material or device and their means of delivery or related materials, including both technologies or dual use goods—
 - (i) for non-legitimate purposes; or
 - (ii) which causes or is likely to cause death or serious injury to any person or substantial damage to property or to the environment;
- (b) an attempt to engage or participate as an accomplice in activities referred to under paragraph (a);
- (c) the provision of technical training, advice, service, brokering or assistance related to any of the activities referred to in paragraphs (a) or (b);
- (d) intentionally and without lawful authority dealing with materials as may be prescribed, which are related to a chemical, biological, radiological or nuclear weapon; or
- (e) intentionally and without lawful authority releasing a dangerous, hazardous, toxic or radioactive substance, microbial or other biological agent or toxin into the environment.

Proliferation Financing means

An act by any person who by any means, directly or indirectly, wilfully provides, gathers, collects, holds or manages funds or other assets, products or rights that can be transformed into funds or other assets, or provides financial services, with the intention that those funds or other assets be used or with knowledge that those funds or other assets may be used in full or in part to finance proliferation.

The Financial Action Task Force Report of 2010 defined proliferation financing as the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations. This definition is of an act of proliferation financing and therefore does not refer to knowledge, intention, or negligence.²² However, the definition of Proliferation Financing in Zambia, which included aspects of knowledge, intention, or negligence, has included all the aspects of this definition.

In the upcoming round of mutual evaluations, countries will be required to demonstrate understanding of their proliferation financing risk. In the context of Financial Action Task Force Recommendation 1, *proliferation financing risk* refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanction obligations referred to in Recommendation 7.

12.1 Potential Breach

Potential Breach means non-compliance with financial sanctions regulations thereby enabling proliferation activities. A potential breach refers to a situation or circumstance that may lead to a violation of regulations, policies, or laws. It is a risk or vulnerability that, if not addressed, could result in an actual breach. Examples include:

- (a) Inadequate customer due diligence processes;
- (b) Insufficient training for employees on AML/CFT procedures; and
- (c) Failure to report suspicious transactions in a timely manner.

12.2 Non-Implementation

Non-Implementation means failure to establish effective controls, allowing sanctioned persons or entities to access financial systems. Non-implementation refers to the failure to put in place required policies, procedures, or controls to comply with regulations. This can be intentional or unintentional. Examples include:

- (a) Not having an AML/CFT policy in place;
- (b) Failing to conduct regular risk assessments; and
- (c) Not designating a Money Laundering Reporting Officer (MLRO).

12.3 Evasion

Evasion means intentional circumvention of sanctions, using techniques like money laundering, shell companies, or false transactions. Evasion involves intentional actions to avoid or circumvent regulations, often with the goal of concealing illicit activities. Examples include:

- (a) Deliberately misleading or deceiving regulators;
- (b) Concealing or destroying evidence of suspicious transactions; and
- (c) Using complex structures or shell companies to disguise ownership or transactions.

The onus therefore is on the entity to ensure that internal processes sufficiently address required standards and that they are adhered to by all employees with sanctions meted out for non-adherence. Collaboration with government entities is essential to keep up with trends and international standards.

The Financial Action Task Force requires countries to implement risk-based measures, commensurate with the risks identified and allocate resources efficiently, to mitigate PF risks, and where countries identify higher risks, they should ensure that their regime to counter PF addresses such risks, including through requiring financial institutions and DNFBSs to take commensurate measures to manage and mitigate the risks. In the case where countries identify lower risks, they should ensure that the measures applied are commensurate with the level of PF risk, while still ensuring full implementation of targeted financial sanctions as required in Recommendation 7. Meanwhile, Supervisors and SRBs should ensure that financial institutions and DNFBSs are implementing their obligations regarding PF risk under Recommendation 1.

12.4 PF Risk Assessment and Mitigation

Financial institutions and DNFBSs are required to identify and assess, their PF risks. FIs DNFBSs should document their PF risk assessments, keep these assessments up to date, and have appropriate mechanisms to provide PF risk assessment information to competent authorities and SRBs. They should also have policies, controls and procedures, which are approved by senior management and consistent with national requirements and guidance from competent authorities and SRBs, to enable them to manage and mitigate the PF risks that have been identified. FIs and DNFBSs should monitor the implementation of those controls and to enhance them if necessary. They should take commensurate measures to manage and mitigate the risks where higher PF risks are identified, (i.e. introducing enhanced controls aimed at detecting possible breaches, non-implementation or evasion of targeted financial sanctions under Recommendation 7), and where the PF risks are lower, ensure that measures to manage and mitigate the risks are commensurate with the level of risk, while still ensuring full implementation of the targeted financial sanctions as required by Recommendation 7³.

12.5 Implementation of Targeted Financial Sanctions

Persons and entities designated by the United Nations Security Council Resolutions (UNSCRs) on proliferation of weapons of mass destruction (WMD) should be identified, deprived of resources and prevented from raising, moving and using funds or other assets for the financing of proliferation. The UN Sanctions list circulated by the NATC is consolidated by the UN to include all known or suspected persons and entities relating to proliferation. The actions required to implement obligations regarding the list are as stipulated under terrorism and terrorism financing.

Targeted financial sanctions should be fully and properly implemented without delay as guided under terrorism and terrorism financing. The Competent authorities will monitor FIs and DNFBSs for compliance. To achieve this, adequate co-operation and co-ordination between the relevant authorities is required in order to develop and implement policies and activities to combat the financing of proliferation of WMD. In this manner, risks of potential breaches, non-implementation or evasion of targeted financial sanctions obligations will be swiftly identified, assessed and understood and risk-based measures to mitigate these risks should be applied to strengthen implementation of targeted financial sanctions.

13.0 Targeted Financial Sanctions Obligations

Targeted financial sanctions for all intents and purposes includes asset freezes, travel bans, financial isolation of designated individuals/entities, and prohibition of proliferation-related transactions. The 2010 Status Report on proliferation financing provides as follows:

13.1 Targeted Financial Sanctions

Targeted financial sanctions can be a positive and effective measure in disrupting WMD proliferation networks. They act not only as a disruptive tool but as a way to provide FIs with proliferation-related information on which they can take action. The disruptive impact of targeted financial sanctions is considered to be most effective when they are implemented globally i.e. by the UN, since the designated entity cannot as easily turn to third-country FIs to evade sanctions. Hence, the UN, as the body responsible for UNSCR 1540 and for ensuring the adoption of effective measures for the worldwide implementation of this Resolution, also has a role in considering the benefits of targeted financial sanctions as a possible avenue for meeting finance-related obligations under UNSCR 1540.

Zambia has enacted the Anti-Terrorism and Non-Proliferation Act to impose targeted financial sanctions on individuals and entities deemed to be involved in WMD proliferation, in line with the sanctions agreed by the UN Security Council.

13.2 UNSCR 1540 and Targeted Financial Sanctions

The general obligation on States is to prevent the activities that UNSCR 1540 describes. UNSCR 1540 does not specifically require states to establish an asset freezing regime. Nevertheless, some jurisdictions have implemented national targeted financial sanctions as a route to meet finance-related obligations under UNSCR 1540. However, UNSCR 1540 primarily requires implementation of export controls, thus no jurisdiction can rely on sanctions alone to meet these obligations. In this regard, the Ministry of Home Affairs and Internal Security prepares a list of restricted goods specified by the Minister, on the recommendation of the Centre, by Gazette notice. Such mechanism is a deliberate measure to control import and export of goods.

13.3 Value of Targeted Financial Sanctions in Counter-Proliferation Efforts

Targeted financial sanctions are particularly effective in addressing proliferation of WMD networks' abuse of the formal financial sector to carry out proliferation-related transactions. Furthermore, the fact that some elements of the proliferation support network may operate for financial gain may make them more susceptible to deterrence by measures that publicly expose them, alerting financial and commercial sectors that they are involved in proliferation activity.

Targeted financial sanctions may also prompt a proliferation-related entity to conceal its involvement in a transaction. This may involve the use of unusual financial mechanisms which may arouse suspicion among legitimate exporters, or patterns of activity which may generate suspicion of money laundering. On the other hand, this may also create particular challenges as it may also make it more difficult for competent authorities to trace and detect proliferation activities.

13.4 Ability of Financial Institutions to Implement Targeted Financial Sanctions

The principal responsibility placed on FIs by targeted financial sanctions is to verify the identity of their customer or counterparty. Therefore entity-based targeted financial sanctions can be implemented effectively by FIs through their use of existing screening systems. Moreover, sanctions lists are an actionable form of information, on the basis of which an FI may freeze an account or refuse a transaction, as required by legislation, involving a listed person or entity without the risk of legal challenge. The quality of lists, intelligence co-operation between jurisdictions, and the effectiveness of de-listing processes following corrective action, have all been identified as important factors in effective use of sanctions.

13.5 Targeted Financial Sanctions as a Supplement to Export Control Regimes

Effective export controls are critical for implementation of UNSCR 1540. Targeted financial sanctions can be a supplement to export control regimes, as export control may not adequately disrupt the financial activities of specific individuals and entities involved in WMD proliferation. While those involved in the illegal export of sensitive proliferation-related items may be prosecuted and convicted under the Act, there may be factual obstacles, e.g. the end-user will typically be in a different jurisdiction which might hamper prosecution. Experience with targeted financial sanctions in other contexts indicates that targeted financial sanctions may provide an avenue to address these difficulties in a counter-proliferation regime, given that they allow for the disruption of a wide range of actors in a proliferation network.

13.6 Implementation of Targeted Financial Sanctions Against Proliferation Finance

Existing FATF guidance on targeted financial sanctions, the Act, SI No. 1 of 2024 and these guidelines are relevant for the implementation of targeted financial sanctions in the non-proliferation context. The legal framework in Zambia has adequate processes for judicial review, listing, and other due processes concerned in the implementation of targeted financial sanctions.

The FATF guidance and Zambia's legal framework also contain valuable provisions to assist competent authorities in implementing targeted financial sanctions imposed multilaterally against proliferation threats. Zambia's legal framework expands the FATF options available to apply targeted financial sanctions to implement the financial obligations of UNSCR 1540.

FIs and DFNBP should note that targeted persons or entities may change their name and thereby escape screening. Hence, attention should be paid to all relevant information provided such as identity numbers, addresses etc on the sanctions list beyond the name only.

13.7 Responsibilities of Financial Institutions

The fundamental element of implementing targeted financial sanctions is Vigilance. FIs and DFNBP should be vigilant by conducting thorough Customer Due Diligence (CDD) and constant account monitoring. However, the nature and depth of CDD undertaken, and how it is organised, can vary significantly between FIs and DFNBP including from transaction to transaction based on the FI's/DFNBP's risk profile.

FIs and DFNBP should conduct risk assessments⁴ and CDD. The purpose of this is to ensure that FIs and DFNBP understand the proliferation financing risks they face and ensure they have the appropriate policies, procedures and processes in place to manage such risks. FIs and DFNBP should follow the procedures listed under section 5.2 of these guidelines to screen the sanctions list for proliferation related persons and entities. The reporting requirements and actions as indicated under terrorism financing equally apply to proliferation financing. Targeted financing sanctions against proliferation and proliferation financing should be implemented without delay and without prior notice.

Ongoing risk-based transaction monitoring would also be beneficial for FIs and DFNBP taking into consideration the National Risk Assessment as well as PF risk indicated listed in Annex 3 beyond persons and entities of concern. The risk of proliferation financing should be part of the established preventive measures and internal controls and integrated with current CDD and risk analysis frameworks. FIs and DFNBP should contact the Centre on any assistance required with regard to PF risk assessment and any other matters incidental hereto. Regular consultations could lead to national improvements in risk analysis that would benefit and protect the financial sector.

13.8 AML/CFTP Regime in Zambia

The Objectives of Zambia's AML/CFTP regime is to prevent money laundering, combat terrorist financing and Proliferation financing (PF), and protect financial system integrity. It is therefore emphasised that key AML/CFTP Regulations include robust mechanisms to facilitate Know Your Customer (KYC), Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), Transaction Monitoring,

Reporting Suspicious Transactions (STR) and appointment of an Anti-Money Laundering Reporting Officer (MLRO). AML/CFT compliance measures should include regular Risk Assessments, Compliance Programs, Training and Awareness programs, Audit and Reviews, and Screening clients against the Sanctions lists provided.

Best Practices have it that FIs and DFNBP should conduct regular Customer risk profiling, Transaction monitoring systems, engage in Information sharing and collaborate with regulators among others as follows:

- (a) Customer Risk Profiling: Assess customer risk based on factors like location, industry, and transaction patterns;
- (b) Transaction Monitoring Systems: Implement automated systems to detect suspicious transactions;
- (c) Information Sharing: Collaborate with other financial institutions and regulators to share intelligence;
- (d) Regulatory Compliance: Stay up-to-date with changing regulations and guidelines;
- (e) Employee Training: Provide regular training on AML/CFT policies and procedures;
- (f) Independent Audit: Conduct regular audits to ensure compliance;
- (g) Risk-Based Approach: Focus resources on high-risk customers and transactions;
- (h) Digital ID Verification: Use digital solutions for customer identification;
- (i) Artificial Intelligence (AI): Leverage AI for transaction monitoring and risk assessment;
- (j) Blockchain Analytics: Utilize blockchain technology for transaction tracking;
- (k) Know Your Employee: Conduct thorough background checks on employees;
- (l) Whistleblower Protection: Establish confidential reporting mechanisms;
- (m) Sanctions Screening: Regularly screen customers and transactions against sanctions lists;
- (n) Beneficial Ownership: Identify and verify beneficial owners; and
- (o) Continuous Monitoring: Regularly review customer relationships;

- (p) Financial Institutions: Implement robust AML/CFT programs;
- (q) Designated Non-Financial Businesses and Professions (DNFBPs): Develop tailored AML/CFT policies;
- (r) Fintech and RegTech: Leverage technology for AML/CFT compliance.

FIs and DNFBPs should keep up to date with evolution of technology and update their systems with Digital ID verification, Artificial Intelligence (AI) in AML/CFT, Blockchain analytics and RegTech solutions.

14.0 *Appeals To The High Court*

A nationally listed person, group or entity that is aggrieved with the decision of the Minister may appeal to the High Court in accordance with the application procedures provided for in Regulation 3 of Statutory Instrument 6 of 1984 [High Court (Appeals) (General) Rules].

15.0 *Contact Details*

All communication shall be directed to the Director General of the NATC using the address provided below:-

The National Anti-Terrorism Centre
P.O. Box 50680 Lusaka, Zambia.
Tel - +260 211 254261/2
info@natc.gov.zm

Annex 1: Glossary

- “competent authority” means an authority with a designated responsibility for combating money laundering, terrorist financing, proliferation financing or associated financial and economic crimes;
- “de-listing” means the removal of a designated person or entity from the targeted sanctions list pursuant to the applicable resolutions, the Act or the Regulations;
- “designated person or entity” means a person or entity designated by the relevant United Nations Security Council Committee;
- “entity” means a person, group of persons, trust partnership, fund or an incorporated association or organisation;
- “freeze” means the prohibition of the transfer, conversion, disposition or movement of funds or other assets that are owned or controlled by a designated person or entity on the basis of, and for the duration of the validity of, an action initiated by the United Nations Security Council or in accordance with applicable Security Council Resolutions by a competent authority or a court;
- “funds” means assets of every kind, whether corporeal or incorporeal, tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets;;
- “funds or other assets” means any assets, including financial assets, economic resources, including oil and other natural resources, property whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, the funds or other assets, including bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts or letters of credit, and any interest, dividends or other income accruing from or generated by the funds or other assets, and any other assets which potentially may be used to obtain funds, goods or services;
- “reporting entity” means an institution required to make reports under this Act which is regulated by a supervisory authority, and includes a financial service provider, a designated non-financial business or profession or a virtual asset service provider;
- “State institution” includes a ministry or department of the Government, a public office, agency, institution, statutory body, commission or company in which the Government or local authority has a controlling interest, other than a State organ;
- “Supervisory Authorities” means —
 - (a) the Bank of Zambia established under the Constitution;
 - (b) the Pensions and Insurance Authority established under the Pension Scheme Regulation Act, 1996;
 - (c) the Securities and Exchange Commission established under the Securities Act, 2016;
 - (d) the licensing committee established under the Tourism and Hospitality Act, 2015;

- (e) the Registrar of Estate Agents appointed under the Estate Agents Act, 2000;
- (f) the Law Association of Zambia established under the Law Association of Zambia Act;
- (g) the Zambia Institute of Chartered Accountants established under the Accountants Act, 2008;
- (h) the Financial Intelligence Centre;
- (i) Chief Registrar of Lands appointed under the Lands and Deeds Registry Act; and
- (j) any other authority established under any written law as a supervisory authority.

“Targeted Financial Sanction” is the act of asset freezing, blocking and rejection of transactions by designated persons or entities or nationally listed persons, groups or entities to prevent, suppress, and disrupt terrorism and its financing as well as the proliferation of WMD and its financing in line with sanctions imposed by the United Nations Security Council (UNSC) through its resolutions

“Terrorism” means —

- (a) an act which constitutes an offence within the scope of, and as defined in one of the applicable treaties specified in Annex 6;
- (b) an act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organisation to do, or to abstain from doing, any act;
- (c) a criminal act that may endanger the life, physical integrity or freedom of, or cause serious injury or death to, any person, group of persons, or causes or may cause damage to public or private property, natural resources, environmental or cultural heritage and is calculated or intended to—
 - (i) intimidate, put in fear, force, coerce or induce the Government, a body, an institution, the general public or any segment thereof, to do or abstain from doing any act, or to adopt or abandon a particular view, or to act according to certain principles;
 - (ii) disrupt any public service, the delivery of an essential service to the public, or to create a public emergency;
 - (iii) create general insurrection in the Republic; or
 - (iv) to threaten diplomatic agents or other internationally protected persons;
- (d) hijacking or unlawfully seizing of an aircraft or public transport or any vessel or the taking of a hostage or group of hostages for ransom;
- (e) unlawful importation, sale, making, manufacture or distribution of any firearms, explosive, ammunition or bomb or generally providing weapons to a terrorist or terrorist organisations;
- (f) an act or omission in or outside the Republic that interferes with an electronic system to harm and cause fear or disrupt the provision of communication, financial, transport or other essential or emergency services to the public for purposes that may include advancing a political, ideological or religious cause;
- (g) arranging for the retention or control of property belonging to a terrorist or terrorist organisation;
- (h) knowingly dealing in property owned or controlled by a terrorist or terrorist organisation;
- (i) soliciting or giving support to a terrorist or terrorist organisation; or
- (j) intentional or unlawful manufacture, delivery, placement, discharge or detonation of any explosive or other lethal device whether attempted or actual, in, into or against a place of public use, a State or government or an organisation, international facility, a public transportation system, or an infrastructure facility with the intent to cause death or serious bodily injury, or extensive destruction likely to or actually resulting in major economic loss;
- (k) traveling outside the Republic for the purpose of perpetrating, planning, or preparation of, or participation in, acts of terrorism, or providing or receiving terrorist training whether against the Republic or any other State;
- (l) seizure, or detention of, or threat to kill, injure or continue to detain a hostage, whether actual or attempted in order to compel a State, an international intergovernmental organisation, a person or group of persons, to do or abstain from doing any act as an explicit or implicit condition for the release of the hostage;
- (m) intentional or unlawful provision or collection of funds or services, or providing or receiving training whether attempted or actual, with the intention or knowledge that any part of the funds or services or training may be used to carry out any of the activities under paragraphs (a) to (l);
- (n) unlawful possession of explosives, ammunition, bomb or any materials for making of explosives, ammunition or bomb for purposes of carrying out any of the activities under paragraphs (a) to (l);
- (o) unlawful possession of materials for promoting an activity under paragraphs (a) to (l) that may include audio or video tapes, written or electronic literature; or
- (p) any promotion, sponsoring, contribution to, command, aid, incitement, encouragement, attempt, threat, conspiracy, organising, or procurement of any person, with the intent to commit any act referred to in paragraph (a) to (o);

“terrorist financing” means an act by any person who wilfully provides or collects funds or other assets, by any means, directly or indirectly, with the intention that those funds or other assets be used, or in the knowledge that they are to be used, in full or in part—

- (a) to carry out an act which constitutes an offence within the scope of and as defined in one of the applicable treaties listed in the Second Schedule;
- (b) to carry out any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organisation to do or to abstain from doing any act;
- (c) to carry out terrorism;
- (d) by a terrorist or by a terrorist organisation, even in the absence of a link to a specific act or acts of terrorism; or
- (e) for the travel of a person to a State other than the person’s State of residence or nationality for the purpose of perpetration, planning or preparation of, or participation in, terrorism or the providing or receiving of terrorist training’.

“without delay” means the implementation of targeted financial sanctions within twenty-four hours, in the case of— (a) designation by the United Nations Security Council or its relevant Sanctions Committee, on designation of the person or entity; or (b) national listing, after listing by the Minister or at the request of another State, as soon as there are reasonable grounds or a reasonable basis to suspect or believe that a person, group or entity meets the criteria for inclusion in the national list. In these Guidelines, a reference to without delay shall be interpreted in the context of the need to prevent the flight or dissipation of funds or other assets, linked to designated persons, groups or entities and the need for coordinated global action to prevent, suppress, interdict and disrupt terrorism, terrorism financing, or the proliferation of weapons of mass destruction and its financing.

Annex 2: Red Flags Indicators

Customer/Client

- (a) Customer/Client has ties to a foreign country of terrorism/proliferation concern, or a neighboring or sympathetic country.
- (b) The customer/client is involved in the supply, sale, delivery or purchase of dual-use, proliferation-sensitive or military goods, particularly to higher risk jurisdictions.
- (c) The customer/client, beneficial owner, or its address or telephone number, is the same or similar to one of the parties found on publicly available lists, including sanctions lists.
- (d) The customer/client is a military or intelligence body connected with a higher risk jurisdiction of terrorism/proliferation concern.
- (e) Customer/client activity does not match the business profile.
- (f) Customer/client is vague, particularly about beneficial owner, end user and end use, provides incomplete information or is resistant to providing additional information when sought.
- (g) Complicated structures to conceal involvement – use of layered letters of credit, front companies, intermediaries and brokers.

Transactions/Orders

- (a) The transaction involves an individual or entity in a foreign country of terrorism/proliferation concern.
- (b) Transaction demonstrates a link between representatives of companies exchanging goods e.g. same owners or management, in order to evade scrutiny of the goods exchanged.
- (c) Transaction involves the shipment of goods inconsistent with normal geographic trade patterns i.e. where the country involved does not normally export or import the types of goods concerned.

Jurisdiction

- (a) Countries with weak financial safeguards and which are actively engaged with a sanctioned country.
- (b) A presence of an industry that produces dual-use goods, proliferation-sensitive items or military goods.
- (c) Deliberate insertion of extra links into the supply chain e.g. diverting shipments through a third country.

Others

- (a) Project financing and complex loans, where there is a presence of other objective factors such as an identified end-user.
- (b) Inconsistencies in information contained in trade documents and financial flows, e.g. names, addresses, final destination.
- (c) Wire instructions or payment from or due to entities not identified on the original letter of credit or other documentation.
- (d) Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.

Annex 3: Indicators of Proliferation Financing Risk

- Transaction patterns
Transactions that involve containers with altered numbers, renamed ships, or goods being shipped on circuitous routes
- Customer risk
Customers involved in the supply, sale, delivery, or purchase of proliferationsensitive, dual-use, or military goods
- Sanctions
Customers or counterparties that are on publicly available sanctions lists, or have addresses that are similar to those on the lists
- Legal and regulatory compliance
Legal and regulatory factors that set standards, requirements, and mechanisms for monitoring and preventing illicit financial activities
- Lapse
An unintentional mistake or oversight, often due to human error.
- Violation
A confirmed breach of regulations or laws.
- Non-compliance
Failure to adhere to regulations, policies, or laws.

This list is not exhaustive as they may be other indicators not listed above. The list only serves as a guide that FIs and DFNBP should look out for among other things specific to their context.

Annex 4: UNSCR 1730 De-listing Procedure (Focal Point)

Petitioners seeking to submit a request for de-listing can do so either through the focal point process outlined below or through their state of residence or citizenship.

The focal point will perform the following tasks:

1. Receive de-listing requests from a petitioner (individual(s), groups, undertakings, and/or entities on the Sanctions Committee's lists).
2. Verify if the request is new or is a repeated request.
3. If it is a repeated request and if it does not contain any additional information, return it to the petitioner.
4. Acknowledge receipt of the request to the petitioner and inform the petitioner on the general procedure for processing that request.
5. Forward the request, for their information and possible comments to the designating government(s) and to the government(s) of citizenship and residence. Those governments are encouraged to consult with the designating government(s) before recommending de-listing. To this end, they may approach the focal point, which, if the designating state(s) so agree(s), will put them in contact with the designating state(s).
6. (a) If, after these consultations, any of these governments recommend delisting, that government will forward its recommendation, either through the focal point or directly to the Chairman of the Sanctions Committee, accompanied by that government's explanation. The Chairman will then place the de-listing request on the Committee's agenda.
- (b) If any of the governments, which were consulted on the de-listing request under paragraph 5 above oppose the request, the focal point will so inform the Committee and provide copies of the de-listing request. Any member of the Committee, which possesses information in support of the de-listing request, is encouraged to share such information with the governments that reviewed the de-listing request under paragraph 5 above.
- (c) If, after a reasonable time (3 months), none of the governments which reviewed the de-listing request under paragraph 5 above comment, or indicate that they are working on the de-listing request to the Committee and require an additional definite period of time, the focal point will so notify all members of the Committee and provide copies of the de-listing request. Any member of the Committee may, after consultation with the designating government(s), recommend de-listing by forwarding the request to the Chairman of the Sanctions Committee, accompanied by an explanation. (Only one member of the Committee needs to recommend de-listing in order to place the issue on the Committee's agenda.) If after one month, no Committee member recommends de-listing, then it shall be deemed rejected and the Chairman of the Committee shall inform the focal point accordingly.
7. The focal point shall convey all communications, which it receives from Member States, to the Committee for its information.

8. Inform the petitioner:

- (a) Of the decision of the Sanctions Committee to grant the de-listing petition; or
- (b) That the process of consideration of the de-listing request within the Committee has been completed and that the petitioner remains on the list of the Committee.

How to submit requests for de-listing:

Please submit requests for de-listing to:

Focal Point for De-listing
Security Council Subsidiary Organs Branch
Room DC2 2034
United Nations
New York, N.Y. 10017
United States of America
Tel. +1 917 367 9448
Fax. +1 917 367 0460
Email: delisting@un.org

Annex 5: UNSCR 2734 De-listing Procedure (Ombudsperson)

In accordance with paragraph 63 of this resolution, the Office of the Ombudsperson shall be authorized to carry out the following tasks upon receipt of a delisting request submitted by, or on behalf of, an individual, group, undertaking or entity on the ISIL (Da'esh) and Al-Qaida Sanctions List or by the legal representative or estate of such individual, group, undertaking or entity ("the petitioner"). The Council recalls that Member States are not permitted to submit delisting petitions on behalf of an individual, group, undertaking or entity to the Office of the Ombudsperson. Information gathering (four months)

1. Upon receipt of a delisting request, the Ombudsperson shall:

- (a) Acknowledge to the petitioner the receipt of the delisting request;
- (b) Inform the petitioner of the general procedure for processing delisting requests;
- (c) Answer specific questions from the petitioner about Committee procedures;
- (d) Inform the petitioner in case the petition fails to properly address the original listing criteria, as set forth in paragraph 2 of this resolution, and return it to the petitioner for his or her consideration; and
- (e) Verify if the request is a new request or a repeated request and, if it is a repeated request to the Ombudsperson and it does not contain relevant additional information, return it to the petitioner, with an appropriate explanation, for his or her consideration.

2. For delisting petitions not returned to the petitioner, the Ombudsperson shall immediately forward the delisting request to the members of the Committee, designating State(s), State(s) of residence and nationality or incorporation, relevant United Nations bodies, and any other States deemed relevant by the Ombudsperson. The Ombudsperson shall ask these States or relevant United Nations bodies to provide, within four months, any appropriate additional information relevant to the delisting request. The Ombudsperson may engage in dialogue with these States to determine:

- (a) These States' opinions on whether the delisting request should be granted; and
- (b) Information, questions or requests for clarifications that these States would like to be communicated to the petitioner regarding the delisting request, including any information or steps that might be taken by a petitioner to clarify the delisting request.

3. Where all designating States consulted by the Ombudsperson do not object to the petitioner's delisting, the Ombudsperson may shorten the information gathering period, as appropriate.

4. The Ombudsperson shall also immediately forward the delisting request to the Monitoring Team, which shall provide to the Ombudsperson, within four months:

- (a) All information available to the Monitoring Team that is relevant to the delisting request, including court decisions and proceedings, news reports, and information that States or relevant international organizations have previously shared with the Committee or the Monitoring Team;

- (b) Fact-based assessments of the information provided by the petitioner that is relevant to the delisting request; and
 - (c) Questions or requests for clarifications that the Monitoring Team would like asked of the petitioner regarding the delisting request.
5. At the end of this four-month period of information gathering, the Ombudsperson shall present a written update to the Committee on progress to date, including details regarding which States have supplied information, and any significant challenges encountered therein. The Ombudsperson may extend this period once for up to two months if he or she assesses that more time is required for information gathering, giving due consideration to requests by Member States for additional time to provide information. Dialogue (two months)
6. Upon completion of the information gathering period, the Ombudsperson shall facilitate a two-month period of engagement, which may include dialogue with the petitioner. Giving due consideration to requests for additional time, the Ombudsperson may extend this period once for up to two months if he or she assesses that more time is required for engagement and the drafting of the Comprehensive Report described in paragraph 8 below. The Ombudsperson may shorten this time period if he or she assesses less time is required.
7. During this period of engagement, the Ombudsperson:
- (a) May submit questions, either orally or in writing, to the petitioner, or request additional information or clarifications that may help the Committee's consideration of the request, including any questions or information requests received from relevant States, the Committee and the Monitoring Team;
 - (b) Should request from the petitioner a signed statement in which the petitioner declares that they have no ongoing association with Al-Qaida, ISIL, or any cell, affiliate, splinter group, or derivative thereof, and undertakes not to associate with Al-Qaida or ISIL in the future;
 - (c) Should meet with the petitioner, to the extent possible;
 - (d) Shall forward replies from the petitioner back to relevant States, the Committee and the Monitoring Team and follow up with the petitioner in connection with incomplete responses by the petitioner;
 - (e) Shall coordinate with States, the Committee and the Monitoring Team regarding any further inquiries of, or response to, the petitioner;
 - (f) During the information gathering or dialogue phase, the Ombudsperson may share with relevant States information provided by a State, including that State's position on the delisting request, if the State which provided the information consents;
 - (g) In the course of the information gathering and dialogue phases and in the preparation of the report, the Ombudsperson shall not disclose any information shared by a state on a confidential basis, without the express written consent of that state; and
 - (h) During the dialogue phase, the Ombudsperson shall give serious consideration to the opinions of designating States, as well as other Member States that come forward with relevant information, in particular those Member States most affected by acts or associations that led to the original listing.
8. Upon completion of the period of engagement described above, the Ombudsperson, shall draft and circulate to the Committee a Comprehensive Report that will exclusively:
- (a) Summarize and, as appropriate, specify the sources of, all information available to the Ombudsperson that is relevant to the delisting request. The report shall respect confidential elements of Member States' communications with the Ombudsperson;
 - (b) Describe the Ombudsperson's activities with respect to this delisting request, including dialogue with the petitioner; and
 - (c) Based on an analysis of all the information available to the Ombudsperson and the Ombudsperson's recommendation, lay out for the Committee the principal arguments concerning the delisting request. The recommendation should state the Ombudsperson's views with respect to the listing as of the time of the examination of the delisting request. Committee discussion
9. After the Committee has had fifteen days to review the Comprehensive Report in all official languages of the United Nations, the Chair of the Committee shall place the delisting request on the Committee's agenda for consideration.
10. When the Committee considers the delisting request, the Ombudsperson, shall present the Comprehensive Report in person and answer Committee members' questions regarding the request.
11. Committee consideration of the Comprehensive Report shall be completed no later than thirty days from the date the Comprehensive Report is submitted to the Committee for its review.

12. After the Committee has completed its consideration of the Comprehensive Report, the Ombudsperson may notify all relevant States of the recommendation.
13. After circulation of the Comprehensive Report to the committee, the Ombudsperson will provide a copy to the State(s) of nationality and residence, the designating State(s), and to those non-Security Council members who participated in the delisting review process by providing substantive information or at any time, upon their request and with the approval of the committee, to any other Member State with a reasonable interest, along with a notification to such States confirming that:
 - (a) All decisions to release information from the Ombudsperson's Comprehensive Reports, including the scope of information, are made by the Committee at its discretion and on a case-by-case basis;
 - (b) The Comprehensive Report reflects the basis for the Ombudsperson's recommendation and is not attributable to any individual Committee member; and
 - (c) The Comprehensive Report, and any information contained therein, should be treated as strictly confidential and not shared with the petitioner or any other Member State without the approval of the Committee.
14. In cases where the Ombudsperson recommends retaining the listing, the requirement for States to take the measures in paragraph 1 of this resolution shall remain in place with respect to that individual, group, undertaking or entity, unless a Committee member submits a delisting request, which the Committee shall consider under its normal consensus procedures.
15. In cases where the Ombudsperson recommends that the Committee consider delisting, the requirement for States to take the measures described in paragraph 1 of this resolution shall terminate with respect to that individual, group, undertaking or entity 60 days after the Committee completes consideration of a Comprehensive Report of the Ombudsperson, in accordance with this annex II, including paragraph 7 (h), unless the Committee decides by consensus before the end of that 60-day period that the requirement shall remain in place with respect to that individual, group, undertaking or entity; provided that, in cases where consensus does not exist, the Chair shall, on the request of a Committee Member, submit the question of whether to delist that individual, group, undertaking or entity to the Security Council for a decision within a period of 60 days; and provided further that, in the event of such a request, the requirement for States to take the measures described in paragraph 1 of this resolution shall remain in force for that period with respect to that individual, group, undertaking or entity until the question is decided by the Security Council.
16. Following the conclusion of the process described in paragraphs 64 and 65 of this resolution, the Committee shall convey, within 60 days, to the Ombudsperson, whether the measures described in paragraph 1 are to be retained or terminated, and approve an updated narrative summary of reasons for listing, where appropriate. In cases where the Committee informs the Ombudsperson that it has followed his or her recommendation, the Ombudsperson immediately informs the Petitioner of the Committee's decision and submits to the Committee, for its review, a redacted version of the Comprehensive Report to be shared with the Petitioner. The Committee reviews the redacted Report within 30 days of the decision to retain or terminate the listing, and communicates its views on the summary to the Ombudsperson. The purpose of the Committee's review is to address any security concerns, including to review if any information confidential to the Committee is inadvertently included in the redacted Report. Following the Committee's review, the Ombudsperson transmits the redacted Report to the Petitioner. The redacted Report shall accurately describe the principal reasons for the recommendation of the Ombudsperson, as reflected in the analysis of the Ombudsperson. In his or her communication with the Petitioner, the Ombudsperson will specify that the redacted Report does not reflect the views of the Committee or of any of its members. In cases where the Committee informs the Ombudsperson that it has not followed his or her recommendation or that the Chair has submitted the question to the Security Council under paragraph 16 of this Annex, the Committee communicates to the Ombudsperson, within 30 days of its decision or the Council's decision, the reasons for this decision for transmission to the Petitioner. These reasons shall respond to the principal arguments of the Petitioner.
17. After the Ombudsperson receives the communication from the committee under paragraph 17 of Annex II, if the measures in paragraph 1 are to be retained, the Ombudsperson shall send to the petitioner, with an advance copy sent to the Committee, a letter that:
 - (a) Communicates the outcome of the petition;
 - (b) Describes, to the extent possible and drawing upon the Ombudsperson's Comprehensive Report, the process and publicly releasable factual information gathered by the Ombudsperson; and
 - (c) Forwards from the Committee all information about the decision provided to the Ombudsperson pursuant to paragraph 17 of Annex II above.
18. In all communications with the petitioner, the Ombudsperson shall respect the confidentiality of Committee deliberations and confidential communications between the Ombudsperson and Member States.
19. The Ombudsperson may notify the petitioner, as well as those States relevant to a case but which are not members of the Committee, of the stage at which the process has reached. Other Office of the Ombudsperson Tasks

20. In addition to the tasks specified above, the Ombudsperson shall:

- (a) Distribute publicly releasable information about Committee procedures, including Committee Guidelines, fact sheets and other Committee-prepared documents;
- (b) Where address is known, notify individuals or entities about the status of their listing, after the Secretariat has officially notified the Permanent Mission of the State or States, pursuant to paragraph 61 of this resolution; and
- (c) Submit biannual reports summarizing the activities of the Ombudsperson to the Security Council.

How to submit requests for de-listing:

You may submit a request for delisting directly to the Office of the Ombudsperson. Legal assistance is not a requirement for the submission of a petition.

Office of the Ombudsperson to the ISIL (Da'esh) and Al-Qaida Sanctions Committee

(DPPA)

UN PO Box 20

New York, NY 10017

United States of America

Tel: +1 212 963 2671

E-mail: ombudsperson@un.org

Content

Your request for delisting should make reference to the relevant entry in the List. Please include the following information:

- (1) Identification information for the petitioner.

— If you are a listed individual, please provide:

- (a) your full name including any middle names or initials, parents' and grandparents' names as may be applicable, as well as any other names or pseudonyms that you use;
- (b) your date and place of birth;
- (c) your nationality - if more than one please provide all;
- (d) your State of current residence; and
- (e) any other information which may help to clarify any issues of identity.

— If you act on behalf of an entity, please provide:

- (a) full name of the entity including any alternative names used;
- (b) if applicable, place and date of incorporation/registration;
- (c) State(s) of current operation(s);
- (d) any other information which may help to clarify any issues of identity; and (e) an explanation of what capacity you are acting on behalf of the entity in.

- (2) A statement of the reasons/justification for delisting.

This section should be as detailed as possible. Please explain why you believe your name should be removed from the list. In particular, you may wish to specify if you:

- contest the existence of some or all facts described in the *Narrative Summary*;
- accept the existence of such facts but argue that they do not establish your association with ISIL (Da'esh) or Al-Qaida; or
- concede that you have been associated with ISIL (Daesh) or Al-Qaida, but you submit that you have disassociated from ISIL (Da'esh) or Al-Qaida or circumstances have changed. In which case, you may wish to explain what steps you have taken to disassociate.

Please address any specific designating criteria set out in the Consolidated List entry or in the Narrative Summary. If, in addition, you have any information or suspicions as to the basis for your inclusion on the list, please include those along with any explanations, arguments or submissions relating to the same.

In order to help you prepare your petition you may wish to check the Ombudsperson's Approach and Standard and the Approach to Analysis, Assessment and Use of Information.

- (3) Where available, copies of any documents or other supporting or explanatory material.
- (4) If applicable, a description of any court proceedings or litigation of relevance to your delisting request.
- (5) If applicable, a reference to any previous request for delisting you have made through the Focal Point or otherwise.

Annex 6: Counter Terrorism Conventions

- 1. The Tokyo Convention on Offences and Certain Other Acts Committed on Board Aircraft of 1963;
- 2. The Convention for the Suppression of Unlawful Seizure of Aircraft of 1970;
- 3. The Montreal Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation of 1971 and the Protocol thereto of 1984;
- 4. The New York Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, including Diplomatic Agents of 1973;
- 5. The International Convention against the Taking of Hostages of 1979;
- 6. The Convention on the Physical Protection of Nuclear Material of 1980;
- 7. The United Nations Convention on the Law of the Sea of 1982;
- 8. The Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation of 1988;
- 9. The Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf of 1988;
- 10. The Convention for the Suppression of Unlawful Acts against Maritime Navigation of 1988;
- 11. The Convention on the Marking of Plastic Explosives of 1991;
- 12. The International Convention for the Suppression of Terrorist Bombings of 1997;
- 13. The Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction of 1977;
- 14. The Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation of 1971;
- 15. The Organisation of African Unity Convention on the Prevention and Combatting of Terrorism, 1999;
- 16. The International Convention for the Suppression of the Financing of Terrorism, 1999;
- 17. The International Convention for the Suppression of Acts of Nuclear Terrorism, 2005;
- 18. The Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, 2005; and
- 19. The Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, 2005.