

Guidelines on Compliance of Government of Pakistan's Notifications issued under United Nations Security Council (UNSC) Resolutions

1. The UNSC's relevant Committee established in pursuance of Resolution 1267 (1999) and successor resolutions approves the addition, amendments and deletion of individuals and entities subject to the assets freeze, travel ban and arms embargo as set out in the aforementioned Security Council resolutions adopted under Chapter VII of the Charter of the United Nations.
2. The UNSC's relevant Committees established in pursuance of resolutions 1718 (2006) and 2231 (2015) and their successor resolutions oversee sanction measures imposed by the UNSC to counter proliferation financing. As a starting point, elements that may indicate potential proliferation financing and sanctions evasion activities are **Annexed**.
3. The Government of Pakistan under the United Nations (Security Council) Act, 1948 gives effect to the decisions of UNSC whenever the Consolidated List maintained by the relevant Sanctions Committee is updated. The Ministry of Foreign Affairs issues Statutory Regulatory Orders (SROs) to provide legal cover for implementing sanction measures under Security Council Resolutions. These SROs in respect of designated¹ individuals/entities require assets freeze, travel ban and arms embargo in addition to other measures in accordance with the Security Council Resolutions. These SROs are also available on the Ministry of Foreign Affairs website.
4. Similarly, for implementing sanction measures under Security Council Resolution 1373 (2001), the Ministry of Interior and respective Home Departments/ Chief Commissioner ICT issues Notifications of proscribed² entities and individuals respectively, pursuant to the Anti-Terrorism Act, 1997.
5. State Bank of Pakistan circulates the subject SROs/ Notifications to its regulated entities for taking necessary action. These SROs/ Notifications, in addition to other requirements, require banks/ DFIs/ MFBs to ensure freezing of assets as per requirements of UNSCRs as reproduced below;

"Freeze without delay the bank accounts, funds and other financial assets or economic resources of these individuals, groups, undertakings and entities, including funds derived from property owned or controlled, directly or indirectly by a proscribed³/ designated individual/ entity, or by persons acting on their behalf or at their direction, and ensure that neither these nor any other funds, financial assets or economic resources are made available, directly or indirectly for such persons' benefit, or by their nationals or by persons within their territory."

SBP also advises its regulated entities to report details of such frozen assets and other action taken in compliance with the relevant SRO/ Notification to SBP within the stipulated time.

¹ Designated under the United Nations (Security Council) Act, 1948

² Proscribed under the Anti-Terrorism Act, 1997

6. Ministry of Foreign Affairs has issued UNSC (Freezing and Seizure) Order, 2019 to streamline the procedure for implementation of Security Council Sanctions against designated individuals and entities. In addition to reporting freeze or seizure of property, banks/DFIs/MFBs have been required to issue notice of seizure or freezing to the concerned designated entity/individual or any other person affected by the freezing as per **Form - B** of the aforementioned Order.
7. To provide further guidance on implementation of the UNSC (Freezing and Seizure) Order, 2019, the Ministry of Foreign Affairs has issued detailed Guidelines for Implementation of UNSC Sanctions, which are available on the Ministry of Foreign Affairs website.
8. Similarly, NACTA has also issued Guidelines on Actions to be taken by Competent Authorities for Implementation of United Nation Security Council Resolution No. 1373, which are available on the NACTA website.
9. The Consolidated Lists available at NACTA's and the UNSC Sanctions Committee's websites, are regularly updated and can be accessed at the following links:
 - (a) https://www.un.org/sc/suborg/en/sanctions/1267/aq_sanctions_list
 - (b) <https://www.un.org/sc/suborg/en/sanctions/1988/materials>
 - (c) <https://www.un.org/sc/suborg/en/sanctions/1718/materials>
 - (d) <http://www.un.org/en/sc/2231/list.shtml>
 - (e) <https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list>
 - (f) <https://nfs.punjab.gov.pk/>

All banks/DFIs/MFBs are advised to regularly access the aforesaid Consolidated Lists to ensure compliance with measures in line with the UNSC resolutions. The updated Consolidated Lists should be accessible down the line in each and every branch or business location. SBP during the course of inspection would check the availability of these updated lists in banks/DFIs/MFBs and action taken there on.

10. Banks/DFIs/MFBs should not provide any banking services to proscribed/ designated entities and persons or their associated persons as required under Anti Money Laundering and Combating the Financing of Terrorism (AML/CFT) Regulations. For this purpose, necessary measures should be taken including but not limited to the following controls:
 - (a) In case of entity accounts, it should be ensured that their beneficial owners, directors, members, trustees and authorized signatories are not linked with any proscribed/ designated entities and persons, whether under the same name or with a different name.

- (b) The association of individuals/ entities with proscribed/ designated entities and persons may be determined on the basis of appropriate screening of sanctions lists/ watch lists, publically known information or linkages on the basis of online NTN verification, government or regulatory sources, reliable media information, etc.
 - (c) While opening new accounts or extending services to customers, any similarity between the identifying information of the customer and that of proscribed/ designated entities and persons including national identification number, address, etc may be viewed with suspicion and properly investigated for necessary action as per requirements.
 - (d) Banks/DFIs/MFBs should monitor their relationships on a continuous basis and ensure that no such relationship exists. If any such relationship is found, immediate action shall be taken as per law, including reporting to the Financial Monitoring Unit (FMU).
11. Banks/ DFIs/ MFBs shall also ensure compliance of subject sanctions regimes with regards to their vendors, employees (permanent, contractual or hired through outsourcing), Board of Directors/ members, sponsors/ shareholders etc.
 12. Banks/DFIs/MFBs shall deploy adequate systems for real time screening and allocate sufficient/trained resources to ensure meticulous compliance of the subject sanctions regimes.
 13. Further, the Government of Pakistan has already prescribed penalty up to Rs. 10 million for non-compliance of sanctions regime under the UN (Security Council) Act, 1948 and the Anti-Terrorism Act, 1997.
 14. The relevant UNSC resolutions permit deposits (credits) in frozen accounts without changing status of the accounts. For further information banks/DFIs/MFBs may access relevant information/documents from the UNSC website.
 15. No charges shall be deducted from such frozen accounts and no such account should be treated as unclaimed deposit for surrendering to SBP. Banks/DFIs/MFBs may seek guidance from Government of Pakistan through SBP regarding any queries on the subject including necessary withdrawals from frozen accounts.
 16. Banks/DFIs/MFBs may educate their customers that in case of any wrongful or inadvertent freezing, they may apply in writing for de-listing to Government of Pakistan through relevant Ministry or to the UN's Ombudsperson, as the case may be.

Situations indicating possible Proliferation Financing Activities

The FATF typologies report on proliferation financing provides a starting point to the public and private sectors in understanding the threats and situations where customers, transactions and other account activities may be involved in proliferation financing. In addition to the aforementioned, national authorities and academic institutions have identified a number of situations below, which may indicate possible proliferation financing activities. However, information below is not uniquely determinative of proliferation financing, and proliferation financing activities may share similar traits with money laundering (especially trade based money laundering) and terrorist financing activities.

Elements that may indicate proliferation financing

- (i) Transaction involves person or entity in foreign country of proliferation concern.
- (ii) Transaction involves person or entity in foreign country of diversion concern.
- (iii) The customer or counter-party or its address is similar to one of the parties found on publicly available lists of “denied persons” or has a history of export control contraventions.
- (iv) Customer activity does not match business profile, or end-user information does not match end user’s business profile.
- (v) A freight-forwarding firm is listed as the product’s final destination.
- (vi) Order for goods is placed by firms or persons from foreign countries other than the country of the stated end-user.
- (vii) Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped, (e.g. semiconductor manufacturing equipment being shipped to a country that has no electronics industry).
- (viii) Transaction involves possible shell companies (e.g. companies do not have a high level of capitalization or displays other shell company indicators).
- (ix) Transaction demonstrates links between representatives of companies exchanging goods i.e. same owners or management.
- (x) Circuitous route of shipment (if available) and/or circuitous route of financial transaction.
- (xi) Trade finance transaction involves shipment route (if available) through country with weak export control laws or weak enforcement of export control laws.
- (xii) Transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.
- (xiii) Transaction involves shipment of goods inconsistent with normal geographic trade patterns (e.g. does the country involved normally export/import good involved?).
- (xiv) Transaction involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws.
- (xv) Based on the documentation obtained in the transaction, the declared value of the shipment was obviously under-valued vis-à-vis the shipping cost.

- (xvi) Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination etc.
- (xvii) Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.
- (xviii) Customer vague/incomplete on information it provides, resistant to providing additional information when queried.
- (xix) New customer requests letter of credit transaction awaiting approval of new account.
- (xx) Wire instructions or payment from or due to parties not identified on the original letter of credit or other documentation.

Potential indicators of sanctions evasion activity

- (i) Involvement of items controlled under WMD export control regimes or national control regimes.
- (ii) Involvement of a person connected with a country of proliferation concern (e.g. a dual-national), and/or dealing with complex equipment for which he/she lacks technical background.
- (iii) Use of cash or precious metals (e.g. gold) in transactions for industrial items.
- (iv) Involvement of a small trading, brokering or intermediary company, often carrying out business inconsistent with their normal business.
- (v) Involvement of a customer or counter-party, declared to be a commercial business, whose transactions suggest they are acting as a money-remittance business.
- (vi) Transactions between companies on the basis of “ledger” arrangements that obviate the need for international financial transactions.
- (vii) Customers or counterparties to transactions are linked (e.g. they share a common physical address, IP address or telephone number, or their activities may be coordinated).
- (viii) Involvement of a university in a country of proliferation concern.
- (ix) Description of goods on trade or financial documentation is nonspecific, innocuous or misleading.
- (x) Evidence that documents or other representations (e.g. relating to shipping, customs, or payment) are fake or fraudulent.
- (xi) Use of personal account to purchase industrial items.
