

NBO's MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM AND SANCTIONS COMPLIANCE POLICY STATEMENT



National Bank of Oman (NBO) is committed to high ethical standards of compliance with the Sultanate of Oman's laws, regulations and guidelines. Our policies on anti-money laundering / Countering Financing Terrorism and Sanctions aims to ensure that risks identified by the bank are appropriately assessed and mitigated.

The requirements described in the AML Policy and Procedures are primarily derived from:

- a) The 40 Recommendations issued by the Financial Action Task Force (FATF) established by countries of the Group of Seven (G7) as detailed in the circulars issued by the Central Bank of the Oman and subsequent amendments issued from time to time.
- b) Royal Decree 30/2016 on Combatting Money Laundering and Terrorism Financing and the related regulations issued by the Central Bank of Oman.

NBO (including its branches and subsidiaries) is committed to implementing single global standards shaped by the most effective anti-money laundering standards available in any location where NBO operates.

NBO has established an Anti-Money Laundering Programme ("AML Programme") for this purpose. The objective of the AML Programme is to ensure that money laundering risks identified by NBO are appropriately mitigated. This is achieved by establishing Board-approved, minimum governing policies, principles, and standards and implementing appropriate controls, to protect NBO, its employees; shareholders and customers from money laundering. The AML Programme provides guidance to all NBO employees, requiring them to conduct business in accordance with applicable AML laws, rules, and regulations.

The AML Programme is based upon various laws, regulations and regulatory guidance from the Regulatory bodies in Sultanate of Oman and, as applicable, other local jurisdictions in which NBO does business/ operate. The Programme includes but is not limited to:

- The appointment of a Money Laundering Reporting Officer ("MLRO") or alternative position as required by local regulation. The Head of Anti Money Laundering is responsible for the establishment of policies and procedures to ensure that the nature of a client's intended activities are recorded and the actual activities are monitored on an on-going basis. The Division Head ensures that the Division's records are sufficient to enable staff to identify unusual and suspicious activities.

1. Customer Due Diligence

- A Customer Due Diligence ("CDD") Programme, which incorporates Customer Identification and Verification ("ID&V") and Know Your Customer ("KYC") principles, and the implementing of programmes designed to appropriately remediate CDD of our existing customers. The line manager is responsible for ensuring that all staff opening accounts and/or on boarding clients have adequate guidance in respect of the Bank's policies and procedures and relevant laws and regulations. The staff member responsible for opening the account and their immediate supervisor are required to identify the beneficial owners of companies and businesses opening accounts or remitting money and to obtain satisfactory evidence of their identities. Before a branch or business unit enters into a banker-customer relationship, the purpose and intended nature of the relationship should be established.
- The Branch or Department maintaining the relationship is responsible for carrying out ongoing customer due diligence on the client relationship and obtain updated information. For example, valid resident card, valid

passport, latest address, residence status, profession/ business, source of funds, etc. Whenever the accuracy of information available is doubted, further customer due diligence should be undertaken.

- Customers and counterparties are regularly screened against lists of terrorists and sanctioned names issued by the Sultanate of Oman, UN, UK HMT, EU and USA by the Sanction Compliance Team through appropriate name filtering systems.
- Conducting enhanced due diligence ("EDD") on customers assessed as higher risk, such as Politically Exposed Persons ("PEPs") in senior positions, their relatives and close associates.
- The Bank prohibits dealing with the following products, services and customer types:
 - a. Anonymous accounts or numbered accounts or customers seeking to maintain an account in an obviously fictitious name
 - b. Shell banks, i.e. banks with no physical presence or staff
 - c. Payable-through-accounts, i.e. NBO does not allow domestic or foreign bank customers to provide payable-through-accounts to their customers on their NBO accounts;

2. Monitoring and Identification of Suspicious Transactions

- Establishing processes and systems designed to monitor customer transactions for the purpose of identifying suspicious activity. Management and staff must use all reasonable efforts to ascertain the expected nature of the client's activities and to monitor this against actual activity.

3. Reporting of Suspicious Transactions

- The Bank is committed to assisting the regulatory authorities in each jurisdiction in which the Bank operates with their efforts to control money laundering and terrorist financing activity.
- All staff is required to report any concerns on account activity or client transactions immediately to their supervisor or the relevant Money Laundering Reporting Officer. For the avoidance of doubt, no manager may forbid a member of staff from raising a concern to the relevant Money Laundering Reporting Officer.
- The Money Laundering Reporting Officer is responsible for the review and the investigation and for subsequent reporting of suspicious activity to the appropriate regulatory bodies as deemed appropriate.

4. Maintaining Records

- It is the Bank's policy to ensure that all client identification documentations, transaction vouchers and other details are maintained for a period of at least 10 years after the closure of the accounts, or last transaction in the case of non-account holders. This may be different for affiliates based in overseas jurisdictions which are subject to local regulatory requirements.

5. Sanctions Screening

- In order to ensure compliance with applicable international financial sanctions, NBO will strive to ensure full transparency on every financial transaction, to screen outgoing and incoming transactions for sanctioned entities or countries, and to review the status of customers from time to time. NBO has a Sanctions Compliance Unit which monitors sanctions issues and the programmes imposed by the Sultanate of Oman, UN, UK HMT, EU and USA. We are committed to complying with all relevant sanctions on every transaction we perform or relationship we maintain.

6. Training

- All staff in client facing or transactions processing areas receive training upon joining the Bank or after transfer to the area and on a regular basis thereafter. The Senior Managers in the branches and business units/department

are responsible for ensuring such training is provided in coordination with the Bank's Human Resource Department.

- The Money Laundering Reporting Officer is responsible for ensuring that training materials and courses meet the required regulatory guidelines in the relevant jurisdiction.

7. Correspondent Banking

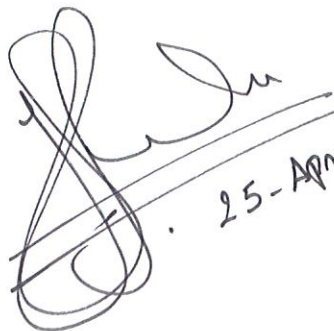
- Obtaining sufficient information on the correspondent to fully understand the nature of its business, its reputation, management and ownership structure and maturity of the bank's regulation and supervision in the respondent's country
- Assessment of the corresponding bank's compliance to regulations and supervision, including assessment of compliance of the respondent bank's AML/CTF systems. Also, assessment of the correspondent's AML and terrorist financing controls
- All correspondent banking relationships are subject to enhanced customer due diligence measures including but not limited to obtaining senior management approval of the onboarding of new correspondent banking relationships.
- Apply transaction monitoring and embargo filtering on transactions with correspondents. NBO will not maintain accounts for shell banks or correspondent banking accounts for banks offering services to shell banks.

Only if the information sought is not available in this policy statement, please send an e-mail request directly to NBO using the following e-mail address: AML@nbo.com

As a supplement to the NBO AML Policy statement we also make available the Wolfsberg Financial Crime Compliance Questionnaire (FCCQ), which gives an overview of basic information about NBO's policies and processes relating to financial crime risk management.

Regards
NBO Compliance




25-Apr-2021