بنك مسقط
bank muscat

Anti-Money Laundering Policy 2019

FOR INTERNAL USE ONLY
Policy owner: DGM Compliance.

Approving Authority	Sign Off/ Approval date
Board of Directors	24th September 2019

Table of contents

1. Introduction

The Anti-Money Laundering (AML) Policy is an expression of bank muscat's commitment to the fight against financial crime and the financing of terrorism. bank muscat will never knowingly allow itself to be used for the purposes of money laundering or terrorist financing. The Board of Directors, Executive Management and the employees of bank muscat, affirm that they shall not in any manner associate themselves with the offences of Money Laundering and Terrorism Financing. Embedding adequate AML/CFT policies and procedures and ensuring appropriate oversight is ultimately the responsibility of the Board of Directors that is cascaded down to Senior Management.

This policy sets outs the Banks principles and minimum standards for Anti-Money Laundering and the financing of terrorism, which must be complied with across all divisions. This Policy sets out these principles and minimum standards to ensure we refer to and follow all applicable laws, rules and industry guidance that are applicable to bank muscat.

The Laws & regulations of the Sultanate of Oman that are applicable in this instant are as follows:

- The Law of Money Laundering, Royal Decree No. 34/2002 dated 27 March 2002;
- CMA Promulgating the Executive Regulation of the Law of Money Laundering, Royal Decree No. 72/2004 dated 28 June 2004;
- Law of Combating Money Laundering and Terrorism Financing dated 8th July 2010;
- Law of Combating Money Laundering and Terrorism Financing issued via Royal Decree No.30/2016 dated 2nd June 2016;
- CBO Circular BM 1152 dated 11th November 2017 regarding Instructions under Law on Combatting Money Laundering and Terrorism Financing (Royal Decree 30/2016);
- Financial Action Task Force (FATF) recommendation.

In order to achieve this and to protect the business, it is essential that Divisions adhere to the AML principles and minimum standards contained herein to ensure effective systems and controls are in place to combat Money Laundering and Terrorist Finance within their areas. The Compliance Department will work closely with each division to ensure the divisional procedures are consistent, up to date and fairly reflect the requirements of this policy.

Abbreviations:

'AML' means Anti-Money Laundering;

'CDD' means Customer Due Diligence;

'CTF' means Combating Terrorist Financing. For the purposes of this Policy, where reference to AML is made, this also refers to CTF;

'MLRO' means Money Laundering Reporting Officer;

'DMLRO' means Deputy Money Laundering Reporting Officer;

'EDD' means Enhanced Due Diligence.

'PEPS' are customers/clients who are Politically Exposed Persons.

'STR' means Suspicious Transaction Report.

'SDD' means Simplified Due Diligence.

'CBO' means Central Bank of Oman.

'ROP' means Royal Oman Police.

'NCFI' means The National Centre for Financial Information.

'Senior Management' means AGMs and above.

2. Definitions

2.1 Definition of Money Laundering

Money laundering occurs every time any transaction takes place or any relationship is formed that involves any form of property that has come from any crime or illegitimate sources. The Criminal offence of money laundering only takes place when both the act of money laundering takes place and the person or business that handles the property has reasonable grounds to suspect that the property derives from crime.

As the term Money Laundering itself indicates, it is a means to wash dirty illegal money and make it clean (legal). It is essentially the process of creating the appearance that large amounts of money obtained from serious crimes, such as drug trafficking, originated from a legitimate source.

2.2 The Money Laundering Process

Money Laundering normally goes through a three stage process consisting of:

Placement: cash form of funds obtained illegally and introduced to the financial systems;

Layering: Putting the deposited cash thorough a complex series of financial transactions in order to disguise the trace of the original source;

Integration: the illegal cash is re-introduced to the economy as proceeds from legitimate sources and washed of all traces of its illegal origins.

2.3 Terrorist Financing

Terrorist financing refers to the processing of funds to sponsor or facilitate terrorist activity. A terrorist group, like any other criminal organization, builds and maintains an infrastructure to facilitate the development of sources of funding, to channel those funds to the providers of materials and or services to the organization, and, possibly, to launder the funds used in financing the terrorist activity or resulting from that same activity.

3. The Money Laundering Reporting Officer

The MLRO is the owner of this Policy and he / she has overall responsibility for providing functional leadership to all Divisions in respect of compliance with the Policy and Minimum Standards.

bank muscat DGM Compliance will hold the position of MLRO within the organization and he / she will be suitably qualified in terms of experience and qualifications to fulfill that role. The MLRO will report directly to the Board and will advise the Board of any material breaches to this policy. In the absence of the MLRO, the Deputy MLRO will ensure the responsibilities of the MLRO are fully executed. The Deputy MLRO will also be suitably qualified in terms of qualifications and AML experience.

Responsibilities of the MLRO are as follows:

- Acts as the contact point in the Bank for the oversight of all activity relating to the prevention of money laundering and terrorist financing;
- Responsible for the communication of the AML Policy to all parts of the business;
- Has a sufficient level of seniority and independence, and is free to act on his/her own authority;
- Has an appropriate compliance framework in place to enable him/her to monitor the day to day operations of the policy and to respond promptly to any reasonable request for information made by the FIU;
- Has sufficient resources to perform all aspects of the role delegated to him;
- Has unfettered access to all relevant information within the organization that will allow him / her to perform his/her role effectively;
- Receiving and considering suspicious transaction reports in relation to knowledge or suspicion of money laundering or terrorist financing activity and making timely external suspicious transaction reports to the National Centre for Financial Information, or relevant law enforcement agencies where appropriate;
- Ensuring adequate arrangements for AML awareness and training are implemented across the Bank;

- Managing the relationship with the regulators in respect of AML matters;

- Providing support to Divisions in relation to drafting procedures to support this policy;

- Providing oversight of compliance with this policy through compliance reviews and reporting the findings to the Board and Executive Management;

- Ensuring the Bank is fully aware of obligations in respect of AML Document Retention obligations;

- Ensuring there are adequate electronic monitoring tools in place to assist with the detection of money laundering and terrorist financing;

- Ensuring all relevant AML regulatory returns are submitted on a timely and accurate basis;

- Ensuring the policy is reviewed on an ongoing basis to ensure it remains fit for purpose and then presenting it to the board for approval at least once every two years.

4. Contact details – Advice and Assistance

If you have any questions regarding any aspect of this Policy please contact the Anti-Money laundering team.

Mr. Fawzi Hamed Al Kiyumi – DGM Compliance, MLRO
FawziAK@bankmuscat.com, Ext 1333

Mr. Muayad Mahmood Bahram, Head of AML, DMLRO
Muayad@bankmuscat.com, Ext 8945

5. Recruitment of AML Staff:

The Recruitment of AML staff will be done in line with the Bank's HR policy. Having this mentioned, the MLRO and/ or the Deputy MLRO will be involved in any staff recruitment for carrying out the AML function.

6. Key guidelines (Articles) as per the Law

Key guidelines (Articles) issued via the Royal Decree 30/2016 dated 2nd June 2016 are as follows. The Bank should ensure continued compliance with all provisions of Law by having the required systems and procedures in place:

Article (6)

"Any person who knew or , should have known or suspected that funds are the proceeds of a crime shall be deemed to have committed the offence of money laundering if he intentionally commits any of the following acts, whether that person had committed the predicate offence or not:

a. *Converts or transfers such funds with the purpose of disguising or concealing the illegal nature or source of such proceeds or of assisting any person who committed the predicate offense to evade punishment for their acts;*
b. *Disguise or conceal the true nature, source, location, method of disposal, movement, or ownership of the funds and their related rights;*
c. *Acquiring, possessing, or using such funds upon receipt."*

bank Muscat Staff should always and continue to report any suspicions of Money Laundering to the MLRO, Deputy MLRO or Compliance AML staff.

Article (8)

"Any person who willingly collects or provides funds, directly or indirectly and by any means, with the knowledge that such funds will be used in full or in part, to carry out a terrorist act, or by a terrorist individual or a terrorist organization, shall be deemed to have committed the offense of terrorism financing.

Such provisions include financing the travelling of individuals to a country other than their country of residence or nationality with the intent to perpetrate, plan, prepare for, participate to or facilitate terrorist acts, or provide necessary funds for training on terrorist acts or receiving such training".

bank Muscat staff should always and continue to report any suspicions in relation to such activities, highlighted in the above article, to the MLRO, Deputy MLRO or Compliance AML staff.

Article (10)

"*Any person who attempts or participates by agreeing, inciting or aiding to commit a money laundering or terrorism financing offence shall be considered an original offender. Legal persons shall be liable for such offence if committed in their name or on their behalf".*

bank muscat staff should take note of the above article and provide the MLRO, Deputy MLRO or Compliance AML staff with any information when it becomes available to them regarding such persons or if they are aware of any Money Laundering/ Terrorist Financing activities occurring in the Bank that is attempted by a customer or another colleague. Staff that disclose such information to the MLRO, Deputy MLRO or Compliance AML staff are protected by virtue of this policy.

Article (33)

"*Financial institutions, non-financial businesses and professions and non- profit associations and entities shall apply due diligence measures, taking into consideration the results of the risk assessment as per the provisions of Article 34 of this law. Due diligence measures include the following:*

a. *Determine and verify the identity of customers based on reliable and independent sources, documents, data and information issued by official authorities in the following cases:*

    1. *Before establishing a business relationship;*
    2. *Before carrying out a transaction for a customer with whom it does not have an established business relationship the value of which is equal to or greater than the threshold specified by the supervisory authority, whether the transaction is executed in a single stage or in multiple stages;*
    3. *Before executing a wire transfer for a customer with whom it does not have an established business relationship the value of which is equal to or greater than the threshold specified by the supervisory authority;*
    4. *When there is suspicion of a crime of money laundering or terrorism financing;*
    5. *When there are doubts concerning the accuracy or adequacy of obtained identification documents and information.*

b. *Identify and verify the identity of any person acting on behalf of the customer and seek proof of the authenticity of their agency according to applicable regulations.*

c. *Identify beneficial owners and take reasonable measures to verify their identity in a satisfactory manner. In the case of legal entities and arrangements, the ownership and control structure of the customer should be understood.*

d. *Know the purpose of the business relationship, and obtain related information as appropriate.*

e. *Continuously update the data and information stipulated in paragraph (a) of this Article related to its customers and beneficial owners whenever necessary, or based on the timeframe specified by supervisory authorities.*

These entities shall also take measures stipulated in the previous paragraphs of this Article for customers and beneficial owners with which the institution had a business relationship upon the entry into force of this law, at times it sees fit, based on materiality and risks".

The Bank's KYC procedure in place that sets the Due Diligence and KYC requirements to be established for different types of customers. In addition, the KYC procedure of the Bank provides the Bank's customer acceptance policy and the negative list of such customers.

Updating of customer information on an ongoing basis is a legal requirement in Oman. This AML policy mandates this requirement. The Bank will put in place the required procedures to ensure customer information is being updated on a regular basis. Such procedure will be based on the AML risk classification of customers by ensuring that high risk customers are updated more regularly that other risk categories customers.

Article (34)

"Financial institutions, non-financial businesses and professions and non- profit associations and entities must comply with the following:

a. *Assess the money laundering and terrorism financing risks in their business, including risks in relation to developing new products and technologies. The risk assessment and its related information shall be documented in writing, kept up-to-date and readily available for competent supervisory authorities to review at their request.*

b. *Establish and implement enhanced due diligence measures in high-risk cases. Entities may identify and conduct simplified due diligence measures in low-*

risk cases, provided that there is no suspicion of money laundering or terrorism financing".

The Bank will continue to conduct a bank-wide risk assessment on AML once every 2 years. This risk assessment will be shared with the Financial Crime Prevention, Ethics and Conflict committee in the Bank. Key risks identified from the risk assessment will be shared with the Board of Directors as part of the Board Quarterly Compliance Report. .

The Bank KYC procedure is put in place to highlight the different due diligence requirements imposed on customers. As a policy, the Bank does not perform simplified due diligence on any customer. The Bank performs normal due diligence on low risk customers from an AML aspect and an enhanced due diligence on high risk customers.

Article (35)

"Financial institutions, non-financial business and professions and non- profit associations and entities must refrain from opening or maintaining anonymous accounts or accounts under fictitious names, numbers or secret codes, or providing any services for such accounts".

As a policy, bank muscat does not and will not open, or maintain anonymous accounts or provide any services for such accounts.

Article (36)

"Financial institutions, non-financial businesses and professions and non- profit associations and entities, must comply with the following:

a. *Monitor and scrutinize all relationships and transactions with customers on an ongoing basis to ensure that information regarding such relationships and transactions are consistent with the information available on the customer, his/her commercial activities and risk profile, and where required, his/her source of funds and wealth. In high-risk cases, enhanced due diligence measures shall be applied and the degree and nature of monitoring increased.*

b. *Examine data and documents obtained from the customer in accordance with Article 33 of this law, to ensure that it is kept up-to-date and consistent with available records.*

c. *Implement specific and adequate measures to address the risks of money laundering and terrorism financing related to non-face-to-face business relationships or transactions for the purpose of identification.*

d. *Establish appropriate risk management systems to determine whether a customer or beneficial owner is a politically exposed person. If the person is a foreign or local politically exposed person, currently or formerly appointed to a prominent position in an international organization, and provided that the business relationship with such person represent a higher risk, entities shall take the following measures:*

    1. *Obtain approval from their senior management before establishing or continuing a business relationship with such person.*
    2. *Take suitable measures to determine the source of his funds.*
    3. *Implement enhanced monitoring of the business relationship.*

e. *Report threshold transactions specified by the supervisory authority to the Centre.*

For the purposes of this Article, politically exposed persons are:

1. *Any natural person currently or formerly appointed to a prominent position in the Sultanate of Oman or a foreign country, members of their family and close associates.*
2. *Any person currently or formerly appointed to a prominent position in an international organization, members of their family and close associates."*

In compliance with the above article, the Bank has established an automated AML system to monitor transactions for an AML aspect. Such transactions monitoring will be verified by the customer's profile and information provided to the Bank. The Bank may also request for additional documentation from customers in order to carry out specific transaction such as SWIFT payment, making large cash deposits and/ or receiving payments from third parties… etc.

The Bank will also establish a mechanism by identifying Politically Exposed persons at account opening stage. This mechanism will involve a self-declaration from the customer and also an automated list matching process through international PEP databases. Please refer to the section of PEPs below for more details on opening accounts for PEPs.

Article (44)

"Financial institutions, non-financial businesses and professions, and non- profit associations and entities shall comply with the following:

a. *Retain all records, documents, information, and data, both domestic and international for a period of at least 10 years after a transaction is carried out. Such records must be sufficient and detailed to facilitate tracking and retrieving every transaction when required according to the provisions of this law.*

b. *Retain records, documents, information, and data obtained through the customer due diligence process under this Chapter, especially account files, business correspondence and the results of any analysis undertaken for at least ten years after the business relationship is ended, or after a transaction is carried out for a customer who is not in an established business relationship with the institution.*

c. *Make such records, documents, information, and data available immediately, upon request, to judicial authorities, the Centre, and supervisory authorities, each within their own jurisdiction. Such entities may and in cases where they deem it necessary, request the extension of the - period specified in this article.*

d. *Financial Institutions, non-financial businesses and professions and non-profit associations and entities may retain certified copies of such original records, documents, information, and data, which shall have the same validity as the originals."*

Refer to page 30

7. AML penalties as per the Royal Decree 30/2016 dated 2nd June 2016:

Penalties:

Article 87

"Without prejudice to a more severe punishment provided for in any other law, the offences specified in this law shall be punishable by the penalties provided therein."

Article 88

"Whoever commits a crime of money laundering shall be punishable by the following:

a. *Imprisonment for a term of not less than 5 years but not exceeding 10 years and with a fine of not less than RO 50,000 but not exceeding the equivalent of the value of the funds subject of the offence, when such person knows or suspects that the funds are proceeds of a crime.*

b. *Imprisonment for a period of not less than six months but not exceeding three (3) years, and a fine of not less than RO 10,000 but not exceeding the equivalent of the value of the funds subject of the offence, when such person should have known that funds are the proceeds of a crime.*

Article 89

Whoever commits a crime of terrorism financing shall be punishable with imprisonment for a term of not less than 10 years and a fine of not less than RO 50,000 but not exceeding the equivalent of the value of the funds collected or provided."

Article 90

"A legal person the responsibility of which has been proven in a crime of money laundering or terrorism financing shall be punishable with a fine of not less than RO 100,000 and not exceeding the equivalent value of funds subject of the offence. The Court may in addition order to suspend its commercial activities permanently or temporarily, close down its headquarter used for the perpetration of the crime, liquidate the business or place it under judicial supervision to manage its funds. The final decree of conviction shall be published through the means of publication."

Article 91

"Any person who attempts or participates by conspiring, abetting or aiding, to commit a money laundering or terrorism financing offence, shall be punished as an original offender."

Article 92

"Penalties stipulated for in this Law shall be doubled in the following cases:

1. *If the offender committed the offence through a criminal organization.*
2. *If the offender committed the offence by abusing his powers or influence through a financial institution or a non-profit or non-governmental organization or the like, or by using the facilities vested in him by his office, professional activity or social status.*
3. *In cases of recidivism."*

Article 95

"A penalty of imprisonment for a term of not less than six months but not exceeding two years and a fine of not less than RO 10,000 but not exceeding RO 50,000, or one of these two punishments, shall be imposed on any of the chairmen and members of the boards of financial institutions, non-financial businesses and professions and non- profit associations and entities, their owners, authorized representatives or employees who, acting intentionally or because of gross negligence, contravene any of the obligations specified in any of the Articles of Chapter Five of this law."

Article 96

"Chairman and members of the boards of financial institutions and non-financial businesses and professions, non-profit associations and entities, their owners, authorized representatives or employees who have failed to comply whether intentionally or by gross negligence with obligations stipulated in Articles 47 and 49 of this Law, shall be punishable with imprisonment for a term of not less than six months but not exceeding three years and a fine of not less than RO 10,000 but not exceeding RO 20,000 or one of these two penalties. If the violation is in the interest or on behalf of a legal person, they shall be punishable with a fine of not less than RO 50,000 but not exceeding RO 100,000."

Article 97

"Any person who intentionally or because of gross negligence fails to comply with obligations stipulated in Articles 30 and 56 of the present Law, is punishable with imprisonment for a term not exceeding two years and a fine not exceeding OR 10,000, or one of these two penalties."

Article 98

"Any person who intentionally or with gross negligence contravenes the provisions of Article 53 of this Law to provide declarations, or by providing false

data or information about currencies or bearer negotiable instruments, or concealing facts that should be disclosed, shall be punishable with imprisonment for a term not exceeding three years and a fine not exceeding RO 10,000 or one of these sanctions. If the violator is a legal person, it should be punishable with a fine of not less than RO 10,000 and not exceeding the value of the funds subject of the crime."

Tipping Off

Special mention is given to Article 49 of the Royal Decree No. 30/2016, which is commonly referred to as "Tipping Off."

"Reporting persons as identified under Article 47 of this Law shall not reveal to the customer, beneficial owner or any other party, directly or indirectly and by any means whatsoever, that they have issued or are about to issue a suspicious transaction report nor should they give any information or data in relation to such reports or alert them to any investigation in this regard."

In order for the Bank to ensure tip-off does not occur, the compliance department's AML team will not disclose information to any other staff or third party regarding details of STRs sent to the NCFI. It should be noted that details of such STRs will only be known to the relevant staff in the compliance department.

8. Principles of Anti-Money Laundering

The senior management of each Division are accountable for managing the AML risks within their Division. They are free to delegate the day-to-day responsibility as they see fit. They are responsible for ensuring effective implementation of, and compliance with, this Policy and supporting procedures i.e. Know Your Customer (KYC) procedure documented by the Bank.

The Policy highlights colleagues' individual obligations / responsibilities and is designed to be directly implemented by each Division.

Each division in bank muscat including International divisions will be responsible for ensuring the following principles and minimum standards have been implemented. The Compliance Department will provide assistance in developing and documenting appropriate procedures that ensure these principles are supported and implemented in a structured fashion.

The following principles are covered in this policy;

- Risk Based approach to AML compliance,
- Customer Acceptance Policy
- Customer Due Diligence H, M, L,
- Persons and Entities subject to Sanctions,
- Politically Exposed Person's,
- Transaction Monitoring,
- Suspicious Transaction Reporting,
- AML Training,
- Record Keeping,
- Monitoring Compliance with policy and procedure.

8.1 Risk Based Approach

bank muscat will adopt a risk based approach to Anti-Money Laundering across a number of specific areas. These areas will be as follows;

- Considering using various levels of identification procedures and collection and/or verification of Customer Due Diligence (CDD) information (e.g. source of funds or wealth); the rationale behind any decision to use Simplified Due Diligence (SDD) or Enhanced Due Diligence (EDD) will be fully documented as part of the banks KYC procedures. All customers will be categorized as High, Medium and Low (H, M, L) risk from an AML perspective,

Further, the following variables or combination of variables could be considered whilst profiling the customer:

- The purpose of the account or relationship;
- The size of deposits or transactions undertaken by a customer;
- The frequency of transactions or duration of the relationship;
- Type of Banking Products taken by the customer

Lower risk or Simplified due diligence (SDD) situations may include the following:

a) Customers, Financial Institutions or non-financial businesses and professions that are subject to requirements to combat money laundering and terrorism financing consistent with the FATF recommendations, have effectively implemented those requirements, and are effectively supervised or monitored to ensure compliance with the requirements;
b) Public companies listed on a stock exchange and subject to disclosure requirements (either by law, or stock exchange rules or other binding

instructions) which impose requirements to ensure adequate disclosure of beneficial ownership;
c) Public administration or enterprises;
d) For products, services, transactions or delivery channels – A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of member's interest under the scheme;

The KYC procedure of the Bank provides the detailed requirements on high risk customers due diligence process based on customer type. The enhanced due diligence may include, but not limited to the following:

a) Answering a dedicated enhanced due diligence related questionnaire;
b) Provide copies of rental agreements and suppliers contracts to verify their business;
c) Obtaining letters from relevant government authorities;

Please refer to the Bank's KYC procedure for more details.

Risk Assessment of customers on the basis of type of customer, products, services and geographic locations:

The Bank adopts a conservative approach and uses the following high level criteria to risk rate its customer base.

- All SAOG customers to be marked as "Low";
- All LLC / trading companies customers with no credit facility to be marked as "High";
- All Asset Management and Private Banking customers to be marked as "High";
- All Politically Exposed Persons (PEPs) to be marked as "High";
- Customers belonging to the following types of accounts will be marked as "High";

    - Non Resident Accounts;
    - Brokers;
    - Finance & Leasing Companies;
    - Money Exchange Companies;
    - Sports, Clubs, Charities & Religious institutions;
    - Educational Institutions / Hospitals;
    - Offshore companies;

- Real Estate business;
- Accountants and Legal Firms;
- Jewelers and precious Metal businesses;
- Cash Intensive customers;
- Corporate customers with complex shareholding structure.

- Customers belonging to the following jurisdictions are marked as "High";

  - Afghanistan
  - Belarus
  - Burma / Myanmar
  - Democratic Republic of Congo
  - Egypt
  - Eritrea
  - Federal Republic of Yugoslavia & Serbia
  - Iran
  - Iraq
  - Ivory Coast
  - Lebanon
  - Liberia
  - Libya
  - Syria
  - North Korea
  - Republic of Guinea
  - Somalia
  - Sudan
  - Tunisia
  - Zimbabwe
  - Rwanda
  - Sierra Leone
  - Russia
  - Yemen
  - Ukraine

Note that the countries are subject to change according to FATF and other international bodies.

The Bank has a detailed Know Your Customer (KYC) procedure in place that covers due diligence requirements for on-boarding various types of customers. All High risk accounts are subject to enhanced due diligence and monitoring. The Bank's KYC procedure provides a detailed due diligence process for all types of accounts;

With regard to product and services, the below are deemed high risk products by the Bank:

Remittance business:

a. In order to mitigate possible AML / sanction risks arising out of remittance business, the Bank has adopted a mechanism to screen and release remittances for high risk jurisdictions;

b. The Bank has documented a detailed Sanctions & matrix document which outlines remittance restrictions to various jurisdictions.

Purchase cases of Housing Loans:

Housing loans are prone to misuse when it comes to money laundering. Hence the compliance department has specific rules in place to detect such misuse through a prepayment of loans. In addition, the compliance department will obtain a regular list from MIS team on prepaid housing loans and review those transactions.

Used cars Auto Loans:

Similar to housing loan, a used car auto loan is prone to money laundering misuse. This is due to the fact that such a product is used to facilitate payments between two individuals rather a reputed card dealer. The compliance department will obtain regular MIS on prepaid used car loans in order to monitor and review same.

Stored value products:

a. The Bank has two stored value products which are prepaid cards and BM Wallet application. Both of these products are deemed high risk from an AML aspect as per the international standards;

b. In order to mitigate risk from the mentioned products, the Bank has introduced controls to only allow funding such products through a bank account. The prepaid card product can only be funded through a bank muscat account whilst the BM wallet can be funded by a bank account or a different wallet all such transactions from account to wallet or account to card are routed through the core banking system and subsequently captured by the AML system through appropriate rules.

Mobile Banking and Internet Banking

a. The majority of STRs sent by the Bank were triggered due to mobile banking and internet banking transactions. Since the nature of these platforms do not involve meeting the customer's face to face prior to conducting a transaction, these two channels are deemed high risk from an AML aspect;

b. In order to mitigate such risks from these mentioned channels, the Bank has put specific rules in place to detect and monitor these transactions.

If an STR has been reported on an account, then relevant customer risk profile will be upgraded i.e. from Low to High or from Medium to High.

For all new products, the AML risk evaluation will be done prior to launch of the product and appropriate monitoring measures will be instilled. This is done thru the Product Approval Committee and is a part of the product evaluation form.

8.2 Customer Acceptance Policy

The Bank does not entertain any walk in customers. To process any transactions in the Bank, the customer should open a bank muscat account. The full details of types of customers allowed/ not allowed to open accounts in the Bank are outlined in the Bank's KYC procedure.

8.3 Customer Due Diligence

bank muscat will ensure the following principles of customer due diligence are followed;

- Verifying the identity of the customer by obtaining documents, data, or information obtained from a reliable and independent source;

- Identifying, where applicable, beneficial owners and taking adequate steps to verify their identity, including in the case of trusts or similar arrangements, to understand the ownership and control structure of the customer;

- Applying enhanced customer due diligence requirements where the risk of money laundering or terrorist financing is higher, taking into account such considerations as non-face-to-face business, non-resident business, PEPs and correspondent banking relationships… etc.;

- Ensuring arrangements are in place for those persons/entities that may (under certain circumstances) not be dealt with (see Persons and Entities subject to Sanctions section);

- Ensuring that no correspondent banking relationships are entered into, or continue with, a shell bank. A shell bank is defined as a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated group;

- Ensuring for the purposes of these minimum standards, the definition of the term 'customer' includes relationships with correspondent banks;

- Ensuring no anonymous accounts are set up for any new or existing customer;

- Ensuring that, if satisfactory evidence of identity cannot be obtained prior to the business relationship commencing, or within a reasonable timescale, the transaction or business relationship must not proceed further;

- Consideration must also be given to whether the failure to produce the standard verification documents merits a report being made to the ROP / CBO or other equivalent agency;

- Ensuring that there is a process of ensuring customers information and supporting documentation is up to date;

- When an existing customer has an account with bank muscat and applies to a separate division to open another account, introductory certificates can be used. Please note that it is the responsibility of both divisions in this instant to ensure that the correct CDD requirements are in place. In addition, divisions should note that these procedures will be subject to additional monitoring from the Compliance team;

- The Bank has a detailed Know Your Customer (KYC) procedure in place that covers due diligence requirements for on-boarding various types of customers. The KYC procedure document, spells out enhanced due-diligence requirements for accounts related to Non-Residents, Charities / Sports Clubs, offshore, Correspondent Banks etc., and all such accounts are required to be pre-approved by Compliance. Further all Asset Management, Private Banking clients are subject to enhanced due diligence and undergo a more

exhaustive account opening / profiling process than the standard account opening process;

- Business Accounts (for any currency) where shareholders are of Iranian, Syrian, Sudanese, Cuban, Russian, Ukrainian, Yemen, Somalia nationality or of a nationality deemed high risk by Compliance need to be pre-approved by Compliance;

- All above accounts are classified as 'High Risk - H' and are subject to enhanced monitoring.

8.4 Persons and Entities that are subject to Sanctions and supporting Terrorist Activities

bank muscat recognize the threat posed by sanctioned entities and individuals to the international banking system. As such, the Bank will take appropriate precautions to ensure there are measures in place to prevent such relationships and to ensure those identified are fully investigated with appropriate action taken. These measures will include the following;

- The Bank will adopt measures to regularly sweep customer transactions against international sanction listings;

- Screening of all outward / inward swift transfers against relevant sanction listings;

- Pre-screening at the account opening stage against international sanction listings;

- Appropriate procedures to determine whether or not a customer identified by the sweep / screening is on a sanctioned listing.

Full details on the sanction listing and steps to be taken once identified are included in the divisional procedures.

8.5 Politically Exposed Persons

As per Royal Decree 30/2016, Combating Money Laundering and Terrorism Financing Law, Politically Exposed Persons are:

1. Any natural person currently or formerly appointed to a prominent position in the Sultanate of Oman or a foreign country, members of their family and close associates.

2. Any person currently or formerly appointed to a prominent position in an international organization, members of their family and close associates.

The terms 'prominent position', 'members of their family' and 'close associates' in Article 36 of the Law should be interpreted to include any natural persons, whether as customer or beneficial owner, who is or was entrusted with a prominent public function in the Sultanate of Oman or in a foreign country, such as Head of States or of governments, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, and important political party officials, or entrusted with a prominent function by an international organisation, such as directors, deputy directors and members of the board. The terms also include immediate family members and close associates. Close associates includes widely and publicly known close business colleagues or personal advisors or any persons who are in position to benefit significantly from close business associations with the politically exposed persons. Family members include the parents, siblings, children, spouse and in-laws of a politically exposed person.

bank muscat recognizes that there is an added risk associated with certain PEP's, and will take appropriate steps that will assist in appropriately managing this business. These measures will include the following;

- Pre- screening of clients to establish if they are Politically Exposed Persons;

- Categorize those that are PEP's on the system;

- The Bank will adopt measures to regularly sweep customer transactions to identify any possible PEP matches;

- Appropriate procedures to determine whether or not a customer identified by the sweep is a PEP;

- Procedures to ensure Senior Management approval for establishing a business relationship with such a person. The level of approval will depend on the risk involved. PEP's in low risk countries, naturally deemed to be lower risk, will be approved by the Compliance function (MLRO and in absence of MLRO then DMLRO) with countries deemed to be higher risk will be approved by the MLRO. In the absence of the MLRO, these will be approved by the

Chief Risk Officer. The categorization of countries is provided in the departmental procedures;

- Non-resident GCC PEPs with a physical presence in Oman such as property ownership, Omani company shareholding… etc. will be subject to the MLRO approval (Deputy MLRO in case of MLRO absence). All other non-residence without a physical presence will be subjected to the relevant business line General Manager approval and the MLRO approval (Deputy MLRO in case of the MLRO's absence);

- Appropriate procedures to ensure ongoing monitoring is performed on such sanctioned identified relationships through the electronic monitoring system.

8.6 Transaction Monitoring

We will ensure that there are procedures in place to monitor customer and staff transactions and activities in order to highlight unusual transactions that may warrant further investigation. We will ensure that scrutiny of transactions is undertaken throughout the course of the relationship to ensure that transactions are consistent with the customer's expected pattern of business.

- bank muscat (Head Office) will perform regular AML assessment to identify those areas of Anti-Money Laundering risk that it is most exposed to. On the back of this it will employ a rules based electronic monitoring tool to ensure customer transactions are monitored, investigated and reported where necessary to the NCIF,

- bank muscat, including its overseas branches must use appropriate transaction monitoring processes. These could take the form of an individual review of a business relationship; manual intervention by colleagues as a result of training and awareness; or the use of automated systems,

- Procedures must ensure that up to date customer information is available to those required to consider analysis of unusual activity so that pertinent questions can be asked and an informed decision made on whether something is suspicious or not,

- Each Division needs to consider the following characteristics when applying a risk based approach as part of their transaction monitoring program:

    - a threshold amount that could be deemed "unusual";

- an abnormal event (e.g. sudden debits or credits out with the normal operation of the account);
- Geographic destinations or origins of payments.

- All training and awareness programs or procedures should include an understanding of the colleague responsibilities in relation to transaction monitoring and situations that could give rise to suspicion.

8.7 Suspicious Transaction Reporting (STR's)

bank muscat fully acknowledges the importance of reporting Suspicious Transactions to the NCIF. The Bank places great emphasis on creating awareness in this area and in ensuring that actual reports are of the required quality before they are furnished to NCFI. The measures the Bank takes to ensure this are as follows:

- The Compliance department will regularly communicate colleague responsibilities in respect of reporting suspicious transactions. It should be noted that all Directors, Management and Employees have a legal duty to report suspicious transactions to the MLRO. Any exchange of information in this regard are protected and kept confidential;

- Colleagues will be allowed to report suspicious transactions to the MLRO directly or via the Anti-Money Laundering team without informing or indeed receiving approval from their line management;

- The compliance department will evaluate all suspicious transactions reported to it and then decide on whether a suspicious transaction report must be furnished to NCFI;

- The compliance department will maintain all suspicious transaction reports furnished to it in a safe and secure location and will not discuss the matter with any colleagues or management outside of the compliance Anti-Money Laundering team;

- The Compliance department will furnish STR's to the NCIF in the prescribed format and ensure this is performed in a clear, concise and speedy fashion. All STR's will be stored in a secure and safe location with access only granted to relevant staff;

- International branches will ensure suspicious reporting complies with local regulatory requirements and the local person assigned with MLRO responsibilities will ensure the branch complies with all regulatory obligations;

- The Compliance department will make all colleagues aware of the penalties / discipline that can be enforced in the event that they do not report suspicious transactions / activity.

8.8 Anti-Money Laundering Training

The MLRO, with the support of L&D, will raise awareness on money laundering and terrorist financing prevention and will train and test relevant colleagues' understanding on what money laundering and terrorist financing is, the requirements of legislation and regulation, relevant KYC procedures, how to recognize and deal with suspicious activity, and the personal obligations of staff. The AML training will be conducted on an annual / on-going basis and is a mandatory requirement for all staff and Board members. The content of the material for staff will include:

  - Topics on Anti Money Laundering;
  - Topics on bribery and fraud;
  - International Sanctions and Sanction Awareness;
  - Politically Exposed Persons;
  - The laws and associated penalties relating to money laundering and terrorist finance and also laws related to specific controls on AML;
  - The recognition and importance of reporting suspicious activity, etc.

- The Bank will have three separate e-learning modules for staff. One dedicated for Senior Management, one for Head Office staff and another for branch staff;
- Board members AML training requirement will be covered as part of the board annual Director training requirements which will include topics related to AML;
- In addition, key staff in the business, control functions and compliance department may be required to sit internationally recognized Certificates in Compliance to ensure there is specialist expertise available in the Bank at all times.

8.9 Record Retention

The Bank will retain adequate records relating to AML, e.g. STR's for at least 10 years and store them in a manner which is secure and easily retrievable. For identification and new customer/account opening records, and all appropriate supporting documentation collated throughout the relationship, these must be retained for at least 10 years after a business relationship has ended. The Bank will respond fully and in a timely manner, to any lawful request for information made by appropriate authorities (e.g. the ROP) during their investigations into financial crime.

8.10 Monitoring Compliance with AML Policy and Divisional Procedures

The Bank will have risk based monitoring plans in place, including monitoring of the account opening process to ensure that all our operations are complying with this Policy and AML Procedures. These monitoring plans will include reviews and audits performed respectively by the Compliance and Internal Audit Departments.

The outcome of these reviews will be reported to Executive Management and the Board of Directors / Board Audit Committee/ Board Risk Committee.

8.11 Updating KYC Information

Customer profiles are captured in the Account Opening Forms (AOF) based on details about the customer like Address, Residential Status, Identity documents, Nature of business activity, Income details etc. The Bank has a process in place to update all customers' information on ongoing basis. In this regard, the Bank has introduced a KYC update form that every customer has to fill during the information update process. Debit card renewal will be used to trigger the first KYC update for individual customers, once the KYC information is received by the bank then the next KYC will be every 3 or 5 years (depending upon the risk classification) from that date or with any subsequent account opening whichever comes first.

The customer update mechanism will be as follows:

- All individual customers classified as low risk or Omanis will be updated once every 5 years;

- All non-Omani individual customers classified as high risk will be updated once every 3 years;
- All corporate customers with credit facilities will be updated once a year based on their credit review process;
- Other Corporate Customers will be updated once their CR expires by Central Operations department through the information provided in Invest Easy.

The Bank may refuse further branch services such as branch transactions, PO, DD, cheque book/ debit card request etc. to customers unless their information is updated. This is to ensure that the customer accounts are updated with the latest information.

8.12 Correspondent Banking

As per the "Guidance on the establishment and maintenance of Foreign Correspondent Banking Relationships" issued by the Wolfsburg group of international banks, "Correspondent Banking is the provision of a current or other liability account, and related services, to another financial institution, including affiliates, used for the execution of third party payments and trade finance, as well as its own cash clearing, liquidity management and short-term borrowing or investment needs in a particular currency". Correspondent Banking relationships are vital in the global payment system, international trade and the global economy as a whole. Correspondent banking relationships are subject to anti-money laundering / counter-terrorist financing / Prevention of Sanctions Evasion measures. The FATF Recommendations require financial institutions to identify and manage the risks associated with these business relationships and to apply specific due diligence measures when they are conducted on a cross-border basis. Hence the bank's KYC procedures stipulate specific due diligence requirements for correspondent banking accounts. Below are the bank's policy requirements in dealing with correspondent banking accounts:

- All new correspondent banking accounts are subject to prior recommendation from compliance department;
- Correspondent banking Vostro accounts should be reviewed at least once a year;
- The Bank will not establish any correspondent relationship or open accounts for Shell banks;
- The Bank will not facilitate Nested Accounts;
- The Bank will not facilitate Payable Through Accounts;
- The Bank will not establish correspondent relationships with entities subject to international sanctions;

The Bank will take steps to terminate correspondent account relationships with those entities which have become subject to international sanctions.

9. Quarterly and Annual Board Reporting

DGM Compliance will present Quarterly Board Compliance report to the Board of Directors at least four times a year, and meet upon request. This report contains a section on all AML matters including the following:

- The number of STRs generated during the quarter and nature of such STRs
- The number of accounts approved/ rejected by compliance and reasons for rejection.
- Evaluation against FATF recommendations and key controls in place;
- Number of Swift Transactions reviewed by Compliance and total number of rejected remittances

Similarly, on an annual basis an annual report is prepared and shared with the board containing statistical information on dormant accounts which provides variations in accounts that has moved out from the dormant category and new accounts that became dormant along with balances.

10. Policy ownership and review

The Policy is owned by DGM Compliance who will ensure that the policy is reviewed on an on-going basis. It will receive Board approval at least once every two years. If there are any material changes to the policy during this time, it will be presented before the Board in the normal course.

11. Assurance

Best practice guidance suggests that the Board of Directors should consider the effectiveness of all policies and procedures on a regular basis. This provides input to the Board's review of the system of internal control. At bank muscat, the internal audit function is mandated to provide assurance in relation to this subject matter.

12. Money Laundering Risk Tolerance

The Bank has zero tolerance on Money Laundering/ Terrorist Financing related matters. Any account that is suspected of money laundering activity will be reported to the NCFI. A call to close accounts that has been reported to the NCFI will be taken by the MLRO of the Bank or would be closed subject to the feedback received from the NCFI. However, if an account is observed to be receiving suspicious foreign payments, or making suspicious payments abroad, such accounts will be blocked from such payments in order to mitigate any correspondent banking risk.