ABU DHABI COMMERCIAL BANK-Egypt (ADCB)

KYC and AML/CFT Guidelines

The objective of the AML/CFT policy is to protect ADCB-Egypt and its group entities by setting clear policy standards to mitigate the risk of ADCB Egypt being unwillingly involved in any activity that may be deemed as related to laundering criminal proceeds or financing terrorism and comply with all relevant regulatory requirements.

This policy sets the duties of Law No. 80/2002 and all other applicable Laws and international recommendations to prevent money laundering and terrorist financing.

Notes:

- The statutory retention period for all records is at least five (5) years
- AML/CFT Training and Development: help in establishing a strong and effective AML/CFT compliance culture including to ensure that the Bank's staff are well-qualified, well-trained, well equipped, and well aware of their responsibility to combat the threat posed by ML/FT. Training scheduled to be made annually unless there is a need for more.
- Our AML/KYC procedures are applicable to all branches of ADCB bank Egypt consider to be complied with the oversight regulations.
- ADCB-Egypt does not provide nesting /downstream correspondent relationships
- ADCB-Egypt does not maintain accounts for offshore banks or Shell banks.

Information to consider about correspondent banks:

The bank collects all the sufficient information about its correspondents to know the nature of works that they execute. The following elements should be available:

1- Collect sufficient information about any receiving correspondent banking institution for the purpose of identifying and achieving a full understanding of the nature of its work, and to make available, through publicly available information, its reputation and level of control, including whether it has been investigated by regulatory, judiciary or law enforcement authorities;
2- Evaluate the anti-crime controls applied by the receiving institution

3- Obtain approval from senior management before establishing new correspondent banking relationships;
4- Information about the management of the correspondent bank, the structure of the main shareholders and the names of executive managers.
5- Assess the money-laundering prevention and detection policies and procedures of the respondent bank
6- clear understanding of the purpose of correspondent banking service provided to the respondent bank

KNOW YOUR CUSTOMER PRINCIPLE

ADCB-Egypt follows a risk-based approach in determining and assessing ML/FT risks associated with its clients, which considers a range of risk factors; and accordingly applies due diligence measures that are commensurate with the level of risks identified. This ensures effective implementation of a risk-based approach, and allows efficient allocation of resources to increase the efficiency of preventative measures.

The best way by which ADCB-Egypt can avoid involvement in money laundering or terrorist financing or other prohibited activities is to have a clear understanding and knowledge of its Client's identities and their practices. The more we know about our Clients, the better positioned we will be to meet regulatory requirements, safeguard the bank's reputation and sell additional products. CDD includes the risk assessment which shall apply to all the parties involved in any relationship, i.e. in addition to the client, joint account holders, authorized signatories, POA holders and partners including ultimate beneficial owners (UBOs).

INDIVIDUALS, ENTITIES AND COUNTRIES WITH WHICH BUSINESS RELATIONSHIP SHALL NOT BE ESTABLISHED

- According to "Know Your Customer Principle" ADCB Egypt do not accept the following categories of customers;

Hawaladars and clients dealing in Hawala Business – Customers who want to open with anonymous or fictitious names – Customers who refuse to provide the required information and documentation – Customers who are included in lists published by international institutions and organizations on the subject of laundering of crime income and terrorism (OFAC, EU, UN, HMT, etc.) – For Retail accounts residents of sanctioned countries – Legal entities that are incorporated in/domiciled in and/or its related individuals are residents of sanctioned countries – In circumstances where identity verification not be undertaken or not

receive sufficient information about the purpose of the business relation – Customers who has a negative record in the bank's internal intelligence system for money-laundering, financing of terrorism, and financial crimes related thereto (fraud, counterfeiting, organized offenses, etc.) – Shell banks, Financial Institutions that deal with Shell banks and Shell Companies – Legal entities/individuals involved in online Gaming or Gambling or Casino businesses - Entities dealing in Virtual Currency/ Crypto Currencies - Legal entities (including the parent companies) with bearer shares structure - Entities involved in manufacturing or trading or dealing in Weapons of Mass Destruction (WMD) and Proliferation of goods and services used in the manufacturing of WMD's

Risk factors for customer risk assessment and risk classification:

- In keeping with risk based approach, ADCB-Egypt has adopted the following risk factors for customer risk assessment and risk classification:
  - Customer Risk o Customer Profile o Employment Details o Source of Funds
  - Jurisdiction Connections o Resident of Egypt o Non-Resident of Egypt
  - Product and Services
  - Channels, and • Reputational Risk

MONITORING AND CONTROL ACTIVITIES

ADCB-Egypt's AML transaction monitoring process is mostly dictated by its suspicious activity monitoring and surveillance software solution which has procedures in place to review, modify and further customize the criteria of the automated monitoring software to generate meaningful alerts on an ongoing basis. The monitoring solution has a set of detection scenarios and risk factors which are parameterized as per the stratification of client portfolio and the risk appetite of the Bank. Each detection scenario is configured to detect a specific pattern of activity and/or risk typologies from Money laundering and Terrorist Financing perspective. Transaction monitoring rules shall be reviewed periodically and tuned accordingly to ensure that they continue to operate as designed. Anti-Money Laundering Unit are the primary users of the monitoring system. Alerts generated by the system are reviewed by the AML analysts, who refer unusual activity to AML investigation and eliminate false positives. The AML investigation team conducts investigation of suspicious activity in a timely and confidential manner and decide on STR filing.

Sanctions:

Before accepting any new customer relationship (or recertifying existing customers as part of the periodic refresh of customer due diligence information), prospective and existing customers, including individuals, legal entities and the beneficial owners/ partners/ senior management/ authorized signatories/ trustees of legal entities, as well as Power of Attorney (POA) must be reviewed (screened) against the internal and external Sanctions Lists in order to rule out the involvement of any Sanctions Target(s).

Before entering into or acceptance of any transaction (remittance investment or trade payment, product or service, together Transactions), the details of each Transaction must be carefully reviewed to include screening the names of all related parties against the Sanctions Lists, in order to mitigate the risk of any Sanctions breach or any other contravention of potentially-applicable Sanctions or this policy