PREVENTION OF MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM AND SANCTION COMPLIANCE– GROUP POLICY

First Abu Dhabi Bank PJSC ("FAB" or "the Bank") is committed to achieving the highest level of compliance with the UAE's laws, regulations and guidelines on Anti Money Laundering (AML) and Counter Financing of Terrorism (CFT) and those of all the jurisdictions in which FAB operates.

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 Central Bank of the United Arab Emirates' (**UAE Central Bank**) Circular No. 24/2000 dated 14/11/2000 and subsequent amendments issued from time to time.

b) Federal Law No. (4) of 2002 regarding Criminalization of Money Laundering.

Where those AML laws, regulations and guidelines set by local authorities differ from those detailed in the Group Policy, FAB overseas branches implement the higher standard or UAEs as appropriate. We also follow the recommendations made in the Wolfsburg Principles on AML in our Private Banking Units.

FAB has a Sanctions Compliance Unit which monitors sanctions issues and the programmes imposed by the UAE, UN, UK HMT, EU and USA. We are committed to complying with all relevant sanctions on every transaction we perform or relationship we maintain.

Customer Due Diligence

The Bank is committed to taking all reasonable efforts to ascertain the true identity of all customers using the Group's services and the source of their funds. FAB's Group Compliance Division is responsible for ensuring that the Bank's policies and procedures comply with relevant laws and regulations in respect of Know Your Customer (KYC) and other client identification requirements.

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.

All staff must take reasonable care to examine any identification and other documents submitted to them to ensure that they are both original and genuine. All staff must take reasonable care to ensure that any photograph presented bears a good resemblance to the person presenting it and where it does not, supplementary documentation should be obtained.

Before a branch or business unit enters into a banker-customer relationship, the purpose and intended nature of the relationship should be established. The unit is responsible for identifying PEPs using commercial databases.

Any power of attorney holder introduced to the Bank must have his identification verified at least to the standard required for an account holder, except if otherwise specifically permitted in the account opening process by quoted companies, government companies etc.

The Bank's policy is that accounts will not be opened for clients without face-to-face contact taking place except with specific approval.

Where accounts are opened by professional intermediaries or introducers, the responsible officer must ensure that the intermediary's policies and procedures comply with (or exceed) the Bank's.

Senior Managers in the branches and business units/departments are responsible for ensuring that their client's on-boarding procedures comply with the Bank's policies.

The Branch or Department responsible for establishing any relationships for high risk accounts should refer to the Head of Prevention Money Laundering and Financial Fraud Department for approval prior to the opening of the account.

The Branch or Department maintaining the relationship is responsible for carrying out on-going customer due diligence on the client relationship and obtain updated information. For example, valid passport, latest address, residence status, profession, 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 UN, US, EU and UAE by the Sanction Compliance Team through appropriate name filtering systems.

Monitoring and Identification of Suspicious Transactions

The Bank is committed to comply with the requirements set by the Regulator in the jurisdiction in which we operate. 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.

The Head of Money Laundering & Financial Fraud 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 base. The Division Head ensures that the Division's records are sufficient to enable staff to identify unusual and suspicious activities.

The Bank uses a dedicated transaction monitoring system to generate alerts of potential suspicious activities for investigation by the PML-FF team.

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 where deemed appropriate onward reporting of transactions to the relevant Central Bank or other authority.

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 5 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.

Payment Screening

In order to ensure compliance with applicable international financial sanctions, FAB 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.

Specific Business and Customers

FAB has established a number of minimum standards in relation to AML controls for high risk customers and businesses which are applicable to all relevant members of the Group.

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 Resources Group.

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