

Policy and Statement on Anti-Money Laundering and Counter-Terrorist Financing

Compliance Department

List of contents

POLICY INFORMATION	3
INTRODUCTION	3
POLICY SCOPE STATEMENT	4
POLICY OBJECTIVES	4
RISK-BASED APPROACH	4

Policy information	
Department/Unit Policy owner	Compliance Department
Policy Description	Anti Money Laundering, Counter Terrorist Financing and Sanction Policy

Introduction

Money laundering and terrorist financing phenomena is considered one of the criminal aspects of major concern to the world for the past years since it is initially associated with organized crimes, especially the drug trafficking, where the criminals benefited from the scale of successive developments in the field of information technology, communications and transportation, in addition to the significant growth in the volume of commercial activities, which led to a huge flow of goods and services amongst different countries.

Money-laundering and terrorist financing crimes are two sides of the same coin. They are in a close relationship, as studies have shown, that most of the funds for terrorism financing were derived from money laundering operations. The criminals took advantage of the global openness and technical development in the banking and financial systems to transfer and move funds around the world hiding their association with criminal or terrorist acts.

The Bank is to abide by and respect all applicable laws and regulations for the conduct of business, wherever it operates. This includes sanctions and restrictions adopted by international organizations (such as the United Nations) or by the sovereign authorities of jurisdictions the Group, directly or indirectly, deals with

Since commercial banks are vulnerable to be missused by criminals for most of the money laundering and terrorist financing crimes, they play an important role by ensuring the adoption and implementation of measures for the prevention, detection, and punishment of the criminals. Banks monitor suspicious activities conducted by the criminals and this requires clear policies and procedures aiming mainly about the bank’s reputation and avoid operational risks that may arise from using thebank as a channel for money laundering. The local laws and regulations and the instructions of the monetary authorities issued in this regard represent the general framework which should be implemented. Furthermore, banks are subject to the global requirements and the international laws which impose conditions on the internal and external banking transactions and correspondent banking relationships.

Policy Scope Statement

This policy applies to all branches of Capital Bank Group, its owned or affiliated companies, operating in the Hashemite Kingdom or abroad (Hereinafter referred to as "Bank") in compliance with the Anti Money Laundering, Counter Terrorist Financing and Sanctions Law and Instructions issued by the Central Bank of Jordan or any other relevant local or international regulators. In case the stated enacted local laws were deemed contradictory at the country where the bank/ branch is operating, then the later shall apply the strickter laws/regulations.

Policy objectives

1. Comply with the Anti Money Laundering and Counter Terrorist Financing Law of the Hashemite Kingdom of Jordan and any other country where the Bank operates.
2. Maintain a strong and and effective Customer Identification program, to manage money laundering and terrorist financing risks, provide assurance to a reasonable extent to regulators, Bank's Board of Directors, and the CEO that the bank complies with the relevant regulatory requirements.
3. Apply global standard and FATF Recommendation related to AML/CTF as well as economic sanction programmms.
4. Protect the Bank from legal, financial and reputation risks.
5. Ensure that the highest standards of integrity are applied when practicing in banking operations in all areas where the bank operates.
6. Take deterrent administrative measures against any employee who violates or ignores Anti Money Laundering and Counter Terrorist Financing policies. Employee who violates policies may be subject to legal accountability from the competent authorities, as stated in the AML laws.
7. The Bank provides legal and professional protection to any employee who reports a suspected operation linked to a money laundering or financing of terrorism activity or any other financial crime.

Risk-based approach

1. The approach is based on the management of money laundering and terrorist financing risks, the approach to commensurate with the nature, size and complexity of the Bank's operations and activities and the level of money laundering and terrorist financing risks, in accordance with its overall risk management framework.
2. A comprehensive AML/CTF risk assessment is carried out annually or when needed, through which the Bank identifies, evaluates and understands the risks, related to customers, , geography, products & services, and operations. The methodology is approved by the Board of Directors.

3. Sanction risks and screening are applied to customers, potential customer, and transactions against local & global Sanction lists to ensure compliance global sanctions programs.
4. Risks are mitigated by applying automation, policies & procedures, training, and monitoring of bank operations.
5. Customer classification is based on risks associated with customer type, ownership structure of the legal person, types of professions, politically exposed persons, geography, citizenship, residency, and products and services, or any other information indicating the level of customer risk.

AML/CTF/Sanctions Program

The bank relies on a risk-based approach in exercising due diligence to comply with combating money laundering, and terrorism financing requirements. Our approach is:

1. Conduct due diligence to identify customers. Due diligence must be conducted prior to establishing a relationship and through out the relationship. The due diligence process must include the identification of the ultimate beneficial owner of the account.
2. The customer and carry out transactions once the identity of the customer, occupation, business activity has been satisfactorily established and verified.
3. The bank prohibit's maintaining or deal with anonymous or numbered accounts, or accounts with fictitious or digital names, or establishing a banking relationship with unidentified individuals, or with shell companies or banks.
4. No account shall be opened until the client's name has been screened against international and local sanctions lists.
5. The bank's policy prohibits directly or indirectly dealings with states, entities, and individuals subject to locan and international sanctions or involved in WMD financing.
6. Agent or authorized person acting on behalf of clients shall be identified, verified, and screened against local and international sanctions lists. Search results should be documented and automatically retrieved when needed.
7. The sources of funds and wealth should be identified and supporting documents obtained.
8. Conduct continuous due diligence on the customers' accounts and monitor the account transactions conducted during the banking relationship and verify that these operations are consistent with the customer's KYC.

AML/CTF/Sanctions Program

9. Ensure that customers' KYCs are regularly updated, and valid identification documents are kept on file.
10. Bank will apply enhanced due diligence when customer poses a higher financial crime risk. The process includes collection additional information/documents to ensure that appropriate controls and the account is within the bank risk tolerance.
11. The bank maintains a policy to measures to idneity and mitigate the risks associated with PEPs, their 1st degree relatives, and known associates.
12. The Bank has a specific due diliegnece process to correspondent relationships risk mitigation and control.
13. The bank implements a monitoring process to review customers transactions and identify complex/unusual transactions. The bank utilizes an automated Transactions Monitoring System and applies risk-based scenarios, rules, and thresholds to identify suspicious activities.
14. The bank screens all customer, potential customers, relevant parties, transaction, and business partners activities against relevant Sanctions lists to ensure compliance.

Banking Operations:

1. The bank does not provide any financial banking services to a natural or legal person who does not have a bank account with the bank.
2. The bank does not provide any services to sanctioned natural or legal persons by the United Nations, National terrorist list, OFAC, EU, UK and other international lists.
3. The bank prohibits customers from using their personal accounts for business purposes, such accounts shall be closed after due notice
4. The bank does not allow payable through , Down streaming/ Upstreaming Clearing, nor Nesting Activities.

Records and Documents Keeping

Records and documents related to local and international operations, as well as due diligence and enhanced due diligence data are documented in an accepted form to the courts for the period prescribed by the supervisory authorities.

AML/CTF/Sanctions Program

Training

An annual training program about anti-money laundering, terrorism financing and sanctions should be established, including the stages of money laundering and terrorism financing, methods of detecting and reporting suspicious activities, and how to deal with suspected customers.