BEINLEUMI
FIRST INTERNATIONAL BANK OF ISRAEL

THE UNIT FOR PROHIBITION OF MONEY LAUNDERING
9, Ahad Ha'am Street, Tel Aviv

May, 2010

Proper Conduct of Banking Business – 411

Formulating a Policy on the subject of
"Prohibition of Money Laundering and Financing of Terror"
The essence of the policy document

Background

On 29 December, 2004, the Knesset passed the **Prohibition of Terrorist Financing Law, 5765-2004**, which formally marks the State of Israel's joining the battle against the financing of international terror.

It is the opinion of all those involved in the subject, including statesmen, jurists, and researchers, that the capability of financing has a decisive effect on the ability to continue to conduct terror activities.

The enactment of the above mentioned law is another component in the series of international treaties for fighting terror and financing terror, as well as associating the subject of financing terror to the battle against money laundering.

It should be noted that since the enactment of the Prohibition of Money Laundering Law and publication of the Order binding on the banking system, the Bank has been implementing a policy of prohibition of money laundering that is reflected mainly in the supervision of the opening of accounts and their management, and monitoring of unusual activity.

Further to the enactment of the above law, the Supervisor of Banks published an Amendment to Proper Conduct of Banking Business – 411 – "Prohibition of Money Laundering and Financing of Terror, and Customer Identification".

Pursuant to the above Amendment, the board of directors of a banking corporation shall set a policy with regard to the "Prohibition of Money Laundering and Financing of Terror", that (according to the wording of the proper conduct directive) "shall include reference also to the monitoring of the threats of money laundering and the financing of terror that arise from modern technology among other things, in particular those that enable transactions to be performed without face-to-face contact, such as the internet, cellular phones, etc. instituting measures to remove those threats".

The policy to be set, as aforesaid, shall be set on a group basis.

The Bank's policy in regard to the prevention of money laundering and financing of terrorism shall make reference to the Bank's ability to scan and detect transactions that may be associated with terrorism financing and to the way the lists of terror organizations and activists as have been declared by other parties may be used.

The policy shall be implemented in addition to the policy that had been formulated by the board of Directors on the subject "Know Your Customer (KYC)" (Enclosed herewith is the wording of the resolution).

It is proposed to set the Bank's policy, according to the following outline, pursuant to the directives of the above mentioned Proper Conduct of Banking Business – 411.

* * * * * * * * * *

a. <u>Customer due-diligence policy</u>

1. The Board of Directors of the Bank shall establish a customer due-diligence policy that, in respect of money laundering and financing of terrorism, shall include reference to the following:

   a. The provision of customer services, including a customer due-diligence procedure when an account is opened or when services are given to a transactor who is not recorded as the owner or authorized signatory of an account;

   b. Classification of high-risk customer groups;

   c. Different customer due-diligence rules for different types of customers;

   d. Monitoring of account activity and heightened monitoring of high-risk customers.

2. While formulating the policy, factors such as the purpose for opening the account, the circumstances under which the account is opened and the intended activity, the customer's area of business, whether he holds a senior public position, the source of his wealth and the money to be deposited in the account, his links with the location of the Bank's branch, whether he was refused service at another financial institution for reasons related to money laundering and terrorism financing, an inquiry regarding his other accounts or

related to his account, and any other detail needed to understand the essence of the customer's activities; in respect of a non-resident – also his links with Israel and whether he is a foreign politically exposed person; and for a business account – a business due-diligence. Profiling of customers and suppliers, and an inquiry into the extent of business activity intended via the account – shall be taken into consideration.

b. Risk Management

The Bank shall incorporate the following basic Know Your Customer principles in its risk management and internal control systems: policy on acceptance of customers, identification of customers, ongoing control of accounts, and of customer's activities not through accounts by various means, in accordance with the extent of exposure to risk.

The Bank shall apply its policy on the prevention of money laundering and financing of terrorism, including risk management, customer-acceptance policy, customer identification procedures, and surveillance of accounts, on a Group basis.

c. Ongoing Monitoring

1. The Bank shall monitor the activities in a customer's account, to assess whether it is consistent with its expectations, on the basis of the customer's declarations, his activity in the account and the banking corporation's acquaintance with the customer, his business activity, his risk profile and, insofar as necessary, the adequacy of the financial sources in the account, etc.
2. The Bank shall operate a computerized system for detecting unusual activities in all its customers' accounts.

3. The Bank shall examine thoroughly whether there is an economic or business reason for complex transactions, or transactions construed in an unusual manner.
4. The Bank shall continue to maintain the procedure that regulates the channels of reporting unusual activities (in accordance with section 9 of the banking Order).

d. <u>High Risk Customer Accounts</u>

1. The Bank established general procedures for defining high risk customer accounts with regard to the prohibition of money laundering and financing of terror.

   The Bank shall apply the current procedure, and shall update it in accordance with the directives of the Proper Conduct of Banking Business. To do so, the Bank shall grade the following factors (which are criteria that affect the definition of high risk customers) into at least two levels:

   The types of the customer's business

   The location of the customer's activity

   The types of services required by the customer

   The types of customers.
2. The Bank shall continue to operate a control system regarding the accounts of these customers.
3. The Bank shall operate an information system that will provide the officer in charge of the unit for prohibition of money laundering with available information that is required for efficient analysis and monitoring of the accounts of high risk customers.
4. A banking corporation shall invoke heightened due-diligence measures vis-à-vis high-risk customers, where a customer who was classified as a high risk customer, wishes to transact a substantial activity, it will require the approval of a senior officer at the Bank.

e. Correspondent Banking

1. The Bank will continue to apply the present policy with respect to engaging in correspondent banking.
2. The Bank shall not engage in correspondent banking with a financial institution which is not supervised with respect to the prohibition of money laundering and financing of terror.
3. The Bank shall not engage in correspondent banking with a bank registered in a jurisdiction where the Bank does not have a physical presence (a 'shell bank'), and shall not engage in business as aforesaid with a financial institution that allows its accounts to be used by a bank of said type.

f. Reporting to the Supervisor of Banks

1. The Bank shall immediately report to the Supervise of Banks, any unusual events that were reported to the competent authority under its reporting requirements, which are material for the stability or reputation of the Bank.
2. The Bank shall immediately report to the Supervise of Banks about any inquiry relevant to money laundering or financing of terror conducted against the bank or a corporation under its control.

g. Transfer of Money and Financial Documents

1. The officer in charge of prohibition of money laundering shall approve any transfer of money through a financial institution in a high risk country, whose final destination is a financial institution in another high risk country, either for it or for one of its customers.
2. The Bank shall operate a computerized database of money transfers from and to high risk countries, which shall provide the officer in charge of the unit for prohibition of money laundering with available information, such as the customer's name and his account number required for detecting and monitoring these transactions, and examining whether they are unusual transactions.

h. <u>Depositing Checks</u>

The Bank shall incorporate rules in its procedures for dealing with the risk inherent in depositing checks, with respect to the prohibition of money laundering and the financing of terror, which shall address the following factors:

1. Endorsed checks drawn on a financial institution abroad
2. Numerous deposits of checks inconsistent with the activity in the customer's account.
3. Checks drawn on a bank outside Israel.

The procedure shall check whether there is a link between the depositing of the check and the execution of a transaction in the Bank, before clearing such a check.

Edited by Konortov Yacov
Head of Compliance