

**PREVENTION OF MONEY LAUNDERING AND FINANCING OF
TERROR, AND CUSTOMER IDENTIFICATION**

Introduction

1. (a) Effective knowledge of banking corporations' customers, including an understanding of the business they conduct with or via the banking corporation, is essential in preventing the banking system from being used for money laundering and financing terror, and for the proper conduct of banking business.
- (b) A banking corporation's involvement in money laundering and the financing of terror is likely to tarnish its reputation and undermine the public's confidence in it and in the whole banking system. Without a thorough examination of a customer's identity, a banking corporation may well be exposed to reputational, operational, legal and other risks. Appropriate know-your-customer (KYC) procedures help to protect a bank's reputation and the integrity of the banking system by reducing the risk of the banking corporation becoming a vehicle for or a victim of financial crime and suffering consequential damage. An adequate KYC policy is therefore essential not only in the battle against money laundering and the financing of terror but also in the maintenance of the stability and credibility of the banking system.

Applicability

2. (a) This regulation shall apply to banking corporations and corporations as specified in sections 11(a)(2) and 11(b) of the Banking (Licensing) Law, 5741–1981 (henceforth, the Licensing Law).
- (b) Notwithstanding the aforesaid in subsection (a),
 - (1) Regarding a foreign bank which a banking corporation controls or in which it is a party at interest,

- (i) If it is subject to the identification obligations relating to the prevention of money laundering, only subsections 25(a) and (b) shall apply.
 - (ii) If it is not subject to the above identification obligations, this regulation, except for sections 9(a), 11, 16(b), 24, 25(c), and 26, shall apply.
- (2) Sections 9(a), 11, 16(b), 24, 25(c), and 26 shall not apply to a branch of a banking corporation outside Israel.
- (c) This regulation shall apply to a foreign corporation which a banking corporation controls or in which it is a party at interest, to the branch of a banking corporation outside Israel, and, with the necessary adjustments, to credit card companies, provided that it does not contravene local laws.

Definitions

3. (a) All terms in this regulation shall have the same meaning as in the Prohibition on Money Laundering (The Banking Corporations' Requirement regarding Identification, Reporting, and Record-Keeping) Order, 5761–2001 (henceforth, the Order), unless stated otherwise.
- (b) In this regulation:
- Officer responsible** — The officer responsible for ensuring that the banking corporation complies with its obligations in accordance with Section 8 of the Prohibiting of Money Laundering Law, 5760–2000.
 - Private banking** — Preferential banking services provided for high net worth customers.
 - High-risk country** — A country or territory classified by the Israel Money Laundering Prohibition Authority (IMPA) as a country or territory to or from which transfers of money require intensified

supervision, that appears in the list in the Appendix to the regulation.

Policy regarding the prevention of money laundering and financing of terror

3. (a) The board of directors of a banking corporation shall set a policy with regard to the prohibition of money laundering and the financing of terror which 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 and cellular phones, instituting measures to remove those threats;
- (b) The policy of the banking corporation with regard to the prohibition of money laundering and the financing of terror shall be set on a group basis, with the required changes, and shall apply for overseas offices, provided that it does not conflict with the local regulations on these subjects.

Know-your-customer (KYC) policy

4. (a) The board of directors of a banking corporation shall set a policy with regard to KYC which, in the matter of money laundering and the financing of terror, shall include reference to the following:
 - (1) Customer acceptance:
 - (2) Definitions of types of customer likely to represent high risk:
 - (3) Different rules for different types of customer.Nothing in this subsection shall prevent the availability of banking services to economically or socially disadvantaged sections of the population.
- (b) In formulating the policy, factors such as the customer's background, his links to Israel and the location of the branch of the banking corporation, his public status, accounts related to his account, the extent of his business activities and the source of his wealth and/or income, etc. shall be taken into consideration.

5. The banking corporation shall allocate authority in an appropriate manner so as to ensure that the policy set by the board shall be implemented

KYC procedures

6. (a) The management of a banking corporation shall determine KYC procedures in accordance with the policy set by the board of directors and with its risk assessment, which will ensure ethical and professional standards that will prevent the banking corporation from being exploited, intentionally or unintentionally, by criminal elements.
- (b) The procedures shall cover, among others, the subjects in this regulation, the reporting system and the staff authorized to handle the reports, the types of record that shall be retained relating to customer identification and to specific transactions, and the period of their retention.

The officer responsible for compliance with the Prohibiting of Money Laundering Law

7. (a) The officer responsible shall be a member of the management of the banking corporation or responsible directly to a member of the management.
- (b) The officer responsible in the banking corporation that heads the banking group shall ensure that the banking corporation's policy and procedures regarding the prohibition of money laundering and the financing of terror is implemented on a group basis.
- (c) The officer responsible shall submit an annual assessment report to the management regarding the implementation of its KYC policy and procedures, in the light of the requirements deriving from the laws, regulations and provisions.

Risk management

8. A banking corporation shall incorporate the following basic KYC principles in its risk-management and internal control systems:

- (a) Customer acceptance;
- (b) Customer identification;
- (c) On-going control of accounts, by using various means (for example, using external data bases) according to the degree of risk exposure.

The banking corporation shall implement the policy regarding the prohibition of money laundering and the financing of terror, including risk management, customer-acceptance policy, customer identification and account monitoring procedures, on a group basis.

Customer identification

9. (a) After opening an account, the banking corporation shall verify the address as recorded in the application form, by sending a notice to the customer at that address confirming the opening of the account. This subsection shall not apply if the customer has requested that notices should not be sent to that address.
- (b) (1) A banking corporation shall not open an account for a customer unless and until it has taken all reasonable steps to determine the true identity of the account holder, the beneficial owners, and the customer's proxies.
- (2) In cases where the account holder or beneficial owner (directly or indirectly) is not an individual, but an individual or group of individuals control it, or are its main beneficiaries, subsection (b)(1) shall apply also to them.
- (3) A banking corporation shall not open an account for a customer who is acting on behalf of a third party and does not provide the information required regarding the third party.
- (c) A banking corporation which has cause to believe that an applicant has been refused banking services by another banking corporation for reasons related to the prohibition on money laundering or the financing of terror shall apply enhanced diligence procedures in opening an account for that customer.

Identification of guarantors

10. Repealed.

Face-to-face identification

11. A banking corporation shall effect identification procedures appropriate to the situations described in Subsections 6(a)(1) to 6(a)(4) of the Order.

Private banking

12. The opening of a new account or changing accounts into private banking accounts in a banking corporation which offers private banking services shall be confirmed by a senior official of the banking corporation.

Retention of identification documents

13. (a) A banking corporation shall establish procedures for the retention of information essential for authenticating customers' identity and their type of business, relating to the source of the information, the period for which it should be retained, the type of customer (individual, company, etc.), and the expected extent of activity in the account. The information shall be retained in a manner which will make it readily available and enable efficient retrieval.

(b) (1) A banking corporation shall undertake reviews to ascertain the existence of adequate and updated information.

(2) The reviews shall take place at times and on occasions determined by the banking corporation in its procedures, such as when a significant transaction is about to take place, or when the requirements relating to customer documentation change, or when the way the account is managed alters significantly.

(3) If a banking corporation discovers that certain significant information about a customer is lacking, it shall take steps to ensure that it obtains the missing information as soon as possible.

On-going monitoring

14. (a) A banking corporation shall monitor activity in a customer's account to assess whether it is consistent with its expectations.

(b) A banking corporation shall operate a computerized system to detect unusual activities in all its customers' accounts. This can be done by setting limits for certain categories of accounts. The banking corporation shall examine thoroughly whether there is an economic or commercial reason for complex transactions or transactions constructed in an unusual manner.

Unusual activities may include transactions that appear to lack economic or business sense, or that involve large sums of money, particularly large cash deposits not consistent with the expected activity in the account.

The Supervisor may exempt a banking corporation from the requirements of this subsection, based on its size, volume of activity and its complexity.

(c) A banking corporation shall set detailed procedures setting out the channel of communications regarding unusual transactions (as per Section 9 in the Order). The procedures should incorporate full documentation of the decision-making process from the first revelation of the unusual transaction to the formulation of a decision on whether to report to the competent authority.

High-risk customer accounts

15. (a) A banking corporation shall include in its procedures rules for defining high-risk customer accounts with regard to the prohibition on money laundering and the financing of terror. To do so the banking corporation shall grade the following factors into at least two levels:

- (1) The type of business (e.g., a cash-intensive business);
- (2) The location of the customer's activity (e.g., a high-risk country, lack of links to Israel);
- (3) The types of services required by the customer (e.g., electronic transfers of large sums);

- (4) The type of customer (e.g., a prominent public figure, an entity with a complex ownership structure).

- (b) A banking corporation shall operate appropriate intensified systems for monitoring these customer's accounts and shall follow up on high-risk accounts by setting key indicators for such accounts, taking note of the background of the customer, the country of origin of the funds, and the type of transactions involved.

- (c) A banking corporation shall operate an adequate information system to provide officers responsible with timely information needed to analyze and effectively monitor high-risk customer accounts. Such reports shall include unusual transactions performed via the customer's account, information on the relationship between the banking corporation and that customer over time, and also information on missing account-opening documentation.

- (d) Significant transactions which customers categorized as high risk wish to perform shall require the approval of a senior manager.

Identification and recording other transactions with customers

- 16. (a) A banking corporation shall authenticate the identities of the parties to a transaction which is likely to constitute a significant risk to the banking corporation.

- (b) A banking corporation shall record the name and identity number of anyone performing a transaction in an account in which he is not registered as an owner or authorized signatory. For the purposes of this subsection, the banking corporation may make do with recording the details given by the person who performed the transaction. In this subsection a transaction means a cash transaction in the amount of less than NIS 10,000 or other transaction in the amount of less than NIS 50,000.

Updating customers' particulars

17. If a customer advises the banking corporation of a change of mailing address:
- (a) The banking corporation shall update the address in all that customer's accounts with the same account number for which the customer originally gave that mailing address, unless instructed otherwise.
 - (b) The banking corporation shall draw the attention of the customer to the need to update the address in his other accounts, if any.

Numbered accounts

18. (a) Numbered accounts (accounts in which the name of the beneficial owner is known to the banking corporation but is substituted by an account number or code name in some documentation) shall be subject to KYC procedures applicable to all accounts.
- (b) The identity of a customer with a numbered account shall be known to a sufficient number of officials to enable a thorough and adequate check of the customer's identity and to monitor his transactions for purposes of identifying unusual activity.
- (c) Numbered account shall not be used to hide a customer's identity from the compliance or supervisory authorities.
- (d) A banking corporation which takes special measures to ensure internal secrecy in regard to customers' accounts shall ensure that the accounts of these customers are examined and monitored at least as thoroughly as accounts of customers regarding whom no such special measures are taken, and shall ensure that the officer responsible and the internal auditors shall have direct access to the information in these accounts.

Third-party accounts

19. (a) A banking corporation shall take the steps required to understand the relationships between the parties related to accounts managed by a trustee (e.g., a legal guardian, liquidator, executor, receiver, attorney, or accountant).

- (b) In the case of a trust which is not established by law, the banking corporation shall record the identification particulars of the trust's founders.

Shares in bearer form

20. A banking corporation shall take special care in dealing with accounts of a company a large part of whose capital or of the capital of the company which controls it consists of shares in bearer form. This subsection shall apply also to accounts of which the said company is a beneficiary.

'Politically exposed' customers (PEPs)

21. (a) On opening an account for a new customer, the banking corporation shall check whether the customer is a public figure.
- (b) The banking corporation shall take steps to discover the source of funds expected to be deposited in the account, before opening an account for a PEP.
- (c) The decision to open an account for a PEP shall be taken by a senior manager.
- (d) The account of a PEP shall be considered a high-risk customer account.

For the purposes of this section, a public figure is a nonresident who holds an important public position abroad, such as heads of state or cities, senior politicians, senior government, judicial or military officials, and officials of political parties, and includes their spouses, and companies under their control.

Correspondent banking

22. (a) A correspondent banking corporation (i.e., one that provides banking services to another banking corporation abroad) shall examine, become familiar with, and understand the nature of its respondent bank's business. As part of the said examination, the banking corporation shall obtain information regarding the respondent bank's main business activities, their location, and its efforts to prevent money laundering and the financing of terror, the purpose for which the account was opened, the condition of banking regulation and supervision in the respondent's country with special reference to the battle against money laundering and the financing of terror.

(b) A banking corporation shall not engage in correspondent banking with a financial institution which is not supervised with regard to the prohibition of money laundering and the financing of terror.

The Supervisor may exempt a banking corporation from the requirements of this subsection, for special reasons.

(c) A banking corporation shall not engage in correspondent banking with a bank registered in a jurisdiction where the respondent bank does not have a physical presence (a 'shell bank') unless it is connected with a supervised banking group.

Training

23. A banking corporation shall provide training on customer identification and KYC, distinguishing between new staff, management staff, branch staff, staff who deal with the acceptance of new customers, and those engaged in compliance, and shall make all employees aware of the procedures it has set.

Non-cooperation by a customer

24. A refusal by a customer to provide details required to enable compliance with the Order, this regulation or the procedures deriving from it, and reasonable grounds for assuming that a transaction is connected with money laundering or the financing of terror, shall be considered reasonable cause for refusal to open and/or manage an account according to the Banking (Service to Customer) Law, 5741-1981.

Reporting to the Supervisor of Banks

25. (a) A banking corporation shall immediately report to the Supervisor of Banks special events reported to the competent authority under its reporting requirements which are essential for the stability or reputation of the banking corporation.

- (b) A banking corporation shall immediately report to the Supervisor of Banks any inquiry relevant to money laundering or the financing of terror being conducted against the banking corporation or a corporation under its control.
- (c) A banking corporation shall report monthly to the Supervisor of Banks on the number and types of reports submitted to the competent authority (the Israel Money Laundering Prohibition Authority).

Registering a public institution, a recognized entity, and a corporation legally established abroad

26. (a) A banking corporation shall allocate an identity number to a public institution according to the Registry of Non-Judicial Entities administered by SHAAM Information Systems in the Ministry of Finance, and the number allocated shall be used for identification purposes by the banking corporation.
- (b) (1) A banking corporation shall allocate a single identity number to a recognized entity and a corporation legally established abroad (for example a central bank) and the number allocated shall be used for identification purposes by the banking corporation.
 - (2) Subsection (1) shall also apply to a public institution not registered in SHAAM which was not allocated an identity number by SHAAM after making an application.

Transfer of money and financial documents

27. (a) Every document of a transfer of cash, securities or other financial assets (including by electronic means such as SWIFT) must include the name of the account holder and the number of the account (in the case of a transfer other than from an account, only the name of the transferor shall be recorded) and the name and account number of the payee.
- (b) The transfer of money via a financial institution in a high-risk country, the final destination of which is a financial institution in another high-risk country,

either for it or for one of its customers, shall be authorized by the banking corporation's officer responsible for the prohibition on money laundering.

- (c) The banking corporation shall operate a computerized database of money transfers from and to high-risk countries which shall make available to the officer responsible information, such as, the customer's name and account number required to detect and monitor these transactions efficiently and to examine whether they are unusual transactions.

Depositing checks

28. The banking corporation shall incorporate rules in its procedures for dealing with the risk related to the prohibition of money laundering and the financing of terror inherent in the deposit of checks, which shall refer to the following, *inter alia*:

- (a) Endorsed checks;
- (b) Numerous deposits of checks inconsistent with the activity in the customer's account;
- (c) Checks drawn on a bank outside Israel. Before clearing such a check, the banking corporation shall ascertain whether there is a link between the depositing of the check and the implementation of the transaction in a banking corporation in Israel.

Appendix

List of high-risk countries and territories

1. Countries or territories which are listed by the FATF (Financial Action Task Force on Money Laundering) as non-cooperative countries or territories in the international war against money laundering.
2. Countries or territories listed in alternative (1) to the definition of "infiltrator" in paragraph 1 of the Prevention of Infiltration Law (Offensive & Jurisdiction) – 1954.
3. The following countries or territories: Afghanistan, Algeria, Iran, Libya, Malaysia, Morocco, Pakistan, The Palestinian Authority, Somalia, Sudan, Tunisia, United Arab Emirates.

* * *