

PREVENTION OF MONEY LAUNDERING AND TERRORISM
FINANCING, AND CUSTOMER IDENTIFICATION

Introduction

1. (a) Money laundering and terrorism financing, as money-intensive activities, are perpetrated via the banking system *inter alia*. Accordingly, banking corporations are at the cutting edge of the struggle to prevent them. Apart from the detriment to values that the relevant legislation protects against, the exploitation of a banking corporation for money-laundering and terrorism-financing activity by criminals or terrorists may tarnish the reputation of, and the public's confidence in, the entire banking system, if not the good name of the State of Israel. Absent thorough examination of the customer's identity and activity and absent the use of effective control and inspection mechanisms, a banking corporation may be exposed to reputational, operational, legal, and other risks. Appropriate customer due-diligence procedures, including understanding the business that the customer conducts via the banking corporation, helps to protect the banking corporation's reputation and the integrity of the banking system by mitigating the risk of the bank's becoming a vehicle for or a victim of financial crime and suffering consequential damage. Therefore, an adequate customer due-diligence policy and ongoing monitoring are essential not only for the war on money laundering and terrorism financing but also for the maintenance of the stability and credibility of the banking system and the country's good name.

Applicability

2. (a) This Directive 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), in a corporation of the kind set forth in Section 11(a)(2) of the Licensing Law, and at a branch of a

ONLY THE HEBREW VERSION IS BINDING

banking corporation outside Israel, the provisions of Sections 11, 16(b), 26, and 31–33 of the Directive shall not apply. In said corporation and said branch, whenever the provisions relating to the prevention of money laundering and terrorism financing in the country where said corporation or branch differ from this Directive, the stricter provisions among them shall apply insofar as they do not contravene the provisions of local law.

Definitions

3. (a) All terms in this Directive shall be construed as in the Prohibition on Money Laundering (Banking Corporations' Requirement regarding Identification, Reporting, and Record-Keeping) Order, 5761–2001 (henceforth, the Order).

(b) In this Directive:

- | | | |
|--|---|--|
| Israel Money Laundering Prohibition Authority | — | The competent authority established by the Minister of Justice under Section 29 of the Prevention of Money Laundering Law, 5760-2000 (hereinafter: the Law). |
| Officer in charge | — | The officer in charge of ensuring that the banking corporation meets its obligations in accordance with Section 8 of the Law. |
| Private banking | — | Preferential banking services provided for high net worth customers. |
| Customer | — | Including a recipient of service. |
| High-risk country | — | A country or a territory included in Appendix 4 of the Order. |
| Banking Corporation | — | As defined in the Licensing Law, and also a corporation as set forth in Sections 11(a)(2) and 11(b) of said Law. |

Prevention of Money Laundering and Financing of Terrorism Policy

- 3a. (a) The board of directors of a banking corporation shall establish a policy in regard to “prevention of money laundering and financing of terrorism.” Said policy shall also address itself to the monitoring of threats to launder money and finance terrorism that originate, among other things, in the use of modern technologies, especially those that facilitate transactions in ways other than face-to-face, e.g., on-line and via cellular telephones, coupled with measures to thwart said threats.
- (a1) A banking corporation’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 (e.g., the UN and the United States Government—OFAC) may be used.
- (b) A banking corporation’s policy in regard to the prevention of money laundering and financing of terrorism shall be established on a group basis, *mutatis mutandis*, and shall apply to overseas branches insofar as it does not clash with local directives in these regards.

Customer due-diligence policy

4. (a) The board of directors of a banking corporation shall establish a customer due-diligence policy that, in respect of money laundering and financing of terrorism, shall include reference to the following:
- (1) 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;
 - (2) classification of high-risk customer groups;
 - (3) different customer due-diligence rules for different types of customers;

(4) monitoring of account activity and heightened monitoring of high-risk customers.

Nothing in this Subsection shall have the effect of withholding banking services from economically or socially disadvantaged population groups.

- (b) In formulating the policy, factors such as the purpose for opening the account, the circumstances under which the account is opened and the activity intended to take place therein, the customer's area of business, whether the customer holds a senior public position, the source of his wealth/income and the money that is to be deposited in the account, his links with the location of the branch of the banking corporation, whether the customer was refused service at a banking corporation for reasons related to money laundering and terrorism financing, an inquiry into accounts related to his account, and any other detail that is needed in order to understand the essence of the account holder's activities; in respect of a nonresident—also his links with Israel and whether the customer is a foreign politically exposed person; and for a business account—also business due diligence, profiling of customers and suppliers, and an inquiry into the extent of business activity intended to be performed via the account—shall be taken into consideration.

5. The banking corporation shall maintain an appropriate division of powers to ensure the implementation of the policy set by the board.

Customer due-diligence procedures

6. (a) The management of a banking corporation shall establish customer due-diligence procedures in accordance with the policy set by the board of directors and with its risk assessment, ensuring ethical and professional standards that will prevent the banking corporation from being exploited, intentionally or unintentionally, by criminal elements.
- (b) The procedures shall cover, *inter alia*, the topics of this Directive, the reporting system and the staff authorized to handle the reports, the types of

records that shall be kept in regard to customer identification and specific transactions, and the period of their retention.

Officer in charge of obligations under the Prevention of Money Laundering Law

7. (a) The officer in charge shall be a member of the management of the banking corporation or a direct subordinate of a member of the management who is not responsible for an area of activity in which business activities take place.
- (a1) The officer in charge shall have a senior formal status at the banking corporation and shall have qualifications, knowledge, and experience commensurate with his duties and purviews.
- (b) The officer in charge at a banking corporation that heads a banking group shall verify, on a group basis, the implementation of the banking corporation's policies and procedures on the prevention of money laundering and financing of terrorism.
- (c) The officer in charge shall present the management and/or the board of directors of the banking corporation, directly, with an annual evaluation report on the application of the banking corporation's policy and procedures regarding customer due diligence, with reference to the assimilation in its own procedures of the obligations imposed by the laws, regulations, and directives, and to the entirety of risks and exposures that the banking corporation faces.
- (d) The officer in charge and his staff shall have unlimited access to all records and information on customer identification and additional customer due diligence documents, transaction documents, and all other relevant information.
- (e) The officer in charge at a branch abroad shall be professionally subordinate to the officer in charge in Israel (and not to the manager of his branch abroad).
- (f) The officer in charge shall verify the employment of a suitably qualified officer in charge at relevant subsidiaries of the banking corporation in Israel and abroad.

Relations with the Internal Audit function

- 7a. (a) The adequacy and efficacy of the working framework of the officer in charge of discharging the banking corporation's obligations under the Prevention of Money Laundering Law shall be subject to periodic review by the Internal Audit function.
- (b) The Internal Audit function shall set aside adequate resources for its review of compliance in this regard (including sample inspections), policies, procedures, and controls.
- (c) The internal auditor at the banking corporation shall advise the officer in charge of the relevant audit findings for the discharge of his duties.

Risk management

8. A banking corporation shall incorporate the following basic customer due-diligence principles into its risk-management and internal-control systems:
- (a) customer-acceptance policy;
- (b) customer identification;
- (c) ongoing control of high-risk accounts by various means (e.g., external databases) in accordance with the extent of exposure to risk.

The banking corporation 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.

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 not be sent to said address.
- (b) (1) A banking corporation shall not open an account for a customer, and shall not add a customer to an existing account, unless 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 rather an individual or group of individuals who control the account or are its main beneficiaries, Subsection (b)(1) shall apply to them as well.
 - (3) A banking corporation shall not open an account for a customer who acts on behalf of a third party and fails to provide requisite information about the third party.
- (c) A banking corporation that has cause to believe that an applicant has been refused banking services by another banking corporation for reasons related to the prohibition against money laundering or financing of terrorism shall apply enhanced diligence procedures before opening an account for said applicant.

Guarantor identification

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 new accounts or the reclassification of existing accounts as private-banking accounts by a banking corporation that 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 needed for the authentication of customers' identity and their type of business. Said procedures shall relate 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 that will make it readily available and efficiently retrievable.

- (b) (1) A banking corporation shall undertake reviews to ascertain the existence of adequate and up-to-date information; A banking corporation shall invoke heightened reviews in accounts of high-risk customers.
- (2) Said 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 changes 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 promptly as possible.

Ongoing surveillance

14. (a) A banking corporation shall apply surveillance of activity in a customer's account in order to assess whether said activity is consistent with its expectations about 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.
- (b) A banking corporation shall operate a computerized system to detect unusual activities in all customer accounts. This may be done by setting restrictions on certain categories of accounts. The banking corporation shall apply heightened scrutiny to determine whether complex or irregularly structured transactions are logical in economic or business terms.
- Unusual activities shall include, *inter alia*, transactions that lack economic or commercial sense, complex transactions, and transactions involving large

sums of money, particularly cash deposits in sums that do not square with the expected activity in the account.

The Supervisor may determine for a banking corporation alternative provisions in lieu of those in this Subsection in consideration of its size, the extent of its activity, and its degree of complexity.

- (b1) A banking corporation shall examine the background and purpose of irregular activity in accounts and shall examine whether said activity constitutes activity that entails reporting under Section 9 of the Order. The findings of said examinations shall be documented in writing and shall be available to the supervisory authorities and the auditors for a period no shorter than seven years.
- (c) A banking corporation shall establish detailed procedures setting out the channel of communications regarding unusual transactions (as per Section 9 in the Order). The procedures shall incorporate full documentation of the decision-making process from first discovery of the unusual transaction to the formulation of a decision on whether to report to the competent authority.
- (d) Reporting on irregular activity under Section 9 of the Order shall take place as promptly as possible under the circumstances of the cast. In the event of special circumstances, an unavoidable delay, or a delay that the banking corporation considers justified, the banking corporation shall document the reasons for said delay.

High-risk customer accounts

- 15. (a) A banking corporation shall include in its procedures rules for defining high-risk customer accounts in respect of the prohibition against money laundering and financing of terrorism. For this purpose, it shall map the following factors at two levels at least:
 - (1) types of customer transactions (e.g., a cash-intensive business);
 - (2) location of customer activity (e.g., high-risk countries, no connection with Israel, etc.);

- (3) types of services required by the customer (e.g., electronic transfers of large sums);
 - (4) type of customer (politically exposed person, entity with a complex ownership structure, etc.).
- (b) A banking corporation shall operate appropriate systems for heightened surveillance of these customers' accounts and shall follow up on high-risk accounts by determining 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 in charge with timely information for the analysis and efficient surveillance of 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 said customer over time, and information on missing account documentation.
- (d) A banking corporation shall invoke heightened due-diligence measures vis-à-vis high-risk customers. Significant transactions that customers categorized as high risk wish to perform shall require the approval of a senior executive.

Identification and recording of other customer transactions

16. (a) A banking corporation shall authenticate the identities of the parties to a transaction that is likely to subject the banking corporation to significant risk.
- (b) (1) 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, the term **“transaction”** denotes a cash transaction in a sum smaller than NIS 10,000 or another transaction in a sum smaller than NIS 50,000.

Updating of 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 said customer's accounts with the same account number for which the customer originally gave said mailing address, unless instructed otherwise.
 - (b) The banking corporation shall call the customer's attention 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 the customer due-diligence procedures that apply 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 detecting unusual activity.
- (c) Numbered accounts shall not be used to hide a customer's identity from the compliance and auditing system or from the supervisory authorities.
- (d) A banking corporation that takes special measures to ensure internal confidentiality in regard to customers' accounts shall ensure that the accounts of these customers are examined and monitored at least as thoroughly as those of customers regarding whom no such special measures are taken, and shall ensure that the officer in charge and the internal auditors will have direct access to information concerning these accounts.

Third-party accounts

19. (a) A banking corporation shall take requisite steps 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 that is not established by law, the banking corporation shall record the identifying 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 also apply to accounts of which said company is a beneficiary.

Politically exposed persons (PEPs)

21. (a) When opening an account for a new customer, the banking corporation shall check whether the customer is a PEP.
- (b) Before opening an account for a PEP, the banking corporation shall take steps to discover the source of funds expected to be deposited in the account.
- (c) The decision to open an account for a PEP shall be taken by a senior executive.
- (c1) If it transpires in the course of the relationship that the customer is a PEP, the decision on continuing the relationship with him shall be made by a senior executive, subject to the provisions of Section 24 below.
- (d) PEP accounts shall be considered high-risk customer accounts.
- (e) Business relations, including account management, with a first-degree relative of a PEP or a corporation controlled thereby, and also with a business partner of a PEP, pose a reputational risk similar to the risks related to the management of business relations, including the management of accounts, with a PEP.

For the purposes of this Section:

Politically exposed person (PEP)—a nonresident who holds a senior public position abroad.

Senior public position—including head of state, president of state, mayor, judge, member of parliament, member of government, high-ranking military or police officer, and any official of said kind even if differently titled.

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 said examination, the banking corporation shall obtain information regarding the respondent bank's main business activities, its location, its efforts to prevent money laundering and financing of terrorism, the purpose for which the account was opened, and the condition of banking supervision and regulation in the respondent's country, with special reference to the war on money laundering and financing of terrorism.
- (b) A banking corporation shall not maintain correspondent relations with a financial institution that is not supervised in regard to the prohibition against money laundering and financing of terrorism.
- The Supervisor may exempt a banking corporation, for special reasons, from the requirements of this Subsection.
- (c) A banking corporation 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") unless it is connected with a supervised banking group, 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.
- (d) Decisions on the conduct of new correspondent relations shall be made by a senior executive.

Training

23. A banking corporation shall provide training on customer identification and due diligence, distinguishing between new staff, management staff, branch staff, staff who deal with the acceptance of new customers and those engaged in compliance, and shall bring the procedures that it has established to all employees' knowledge. Said training shall be performed on an ongoing basis in order to assure that the information in the hands of staff is up to date and includes information on the

latest techniques, methods, and trends. In the training, special attention shall be devoted to all provisions relating to the prevention of money laundering and financing of terrorism and, in particular, to requirements concerning the reportage of irregular transactions. The banking corporation shall take such actions as are needed to assimilate the knowledge.

- (b) A banking corporation shall establish procedures assuring the maintenance of high standards for the hiring of new staff commensurate with the nature of the job.
- (c) For the purposes of this Section, "**staff**" includes employees of personnel companies.

Non-cooperation by a customer

24. Refusal by a customer to provide details required to facilitate compliance with the Order, this Directive, and the procedures deriving from, as well as reasonable cause to assume that a transaction is related to money laundering or financing of terrorism, shall be considered reasonable cause for refusal to open and/or manage an account and to provide services for a transactor who is not recorded as the owner or authorized signatory of the account for the purposes of the Banking (Service to Customer) Law, 5741–1981. In such a case, the banking corporation shall consider the possibility of presenting the competent authority with an irregular-activity report (under Section 9 of the Order).

Reporting to the Supervisor of Banks

25. (a) A banking corporation shall immediately report to the Supervisor of Banks about special events that were reported to the competent authority under reporting obligations that are essential for the stability or reputation of the banking corporation.
- (b) A banking corporation shall immediately report to the Supervisor of Banks about any investigation with implications related to money laundering or financing of terrorism that is being conducted against the banking corporation or a corporation under its control.

- (c) A banking corporation shall report on a monthly basis to the Supervisor of Banks about the number and types of reports submitted to the competent authority (the Israel Money Laundering Prohibition Authority).
- (d) A banking corporation shall report to the Supervisor of Banks whenever a foreign corporation that the bank controls, or in which it has a substantial interest, or a branch of a banking corporation outside Israel, does not act in accordance with this Directive because the Directive contravene the provisions of local laws.

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 (e.g., a central bank) and the banking corporation shall use the number allocated for identification purposes.
- (2) Subsection (1) shall also apply to a public institution not registered with SHAAM that was not allocated an identity number by SHAAM after making an application.

Transfers of funds and financial documents

- 27. (a) A transfer of funds by means of a financial institution in a high-risk country, in which the final destination is a financial institution in another high-risk country—for said institution or for its customer—shall entail approval by the official at the banking institution who is in charge of the prohibition against money laundering.
- (b) A banking institution shall operate a computerized system of information on transfers of funds among high-risk countries. Said system shall provide the

official in charge with readily available information about customers' names and account numbers, among other things, as are needed for the detection and efficient surveillance of such transactions and determination of whether they are irregular.

Deposit of checks

28. A banking corporation shall establish, in its procedures, rules for dealing with the risk present in a transaction of deposit of checks in the context of the prohibition against money laundering and financing of terror, with reference to the following factors *inter alia*:

- (a) endorsed checks;
- (b) depositing of many checks that are not consistent with activity in the customer's account;
- (c) checks drawn on a bank outside of Israel. In such a case, before clearing takes place, the banking corporation shall verify the existence of a relationship between the depositing transaction and the performance of the transaction with a banking corporation in Israel.

Countries deficient in applying FATF recommendations

29. A banking corporation shall make sure that branches and corporations under its control in countries that do not adequately apply FATF recommendations, honor the provisions of the Directive insofar as said provisions do not contravene local laws and regulations.

Financial Activity vis-à-vis banks operating in the Palestinian Authority areas

30. A banking Corporation shall not accept for deposit checks, in domestic or foreign currency, that are drawn on banks that operate in the Palestinian Authority areas, if the identifying particulars of the account owner/s are not printed thereon in Latin characters and in digits customarily used in the state of Israel.

31. A banking corporation shall not accept checks for collection, in domestic or foreign currency, that are presented by banks that operate in the Palestinian Authority areas without obtaining the particulars of the account in which the check was deposited and the identifying particulars of all owners of said account, in Latin characters and in digits customarily used in the state of Israel.
32. A banking corporation shall not accept for deposit endorsed checks drawn on banks operating in the Palestinian Authority areas and shall not accept for collection endorsed checks presented by banks that operate in the Palestinian Authority areas.
33. A banking corporation shall not accept a transfer of funds in a sum exceeding NIS 5,000 from banks operating in the Palestinian Authority areas without obtaining the particulars of the account of the counterparty to the transaction and the identifying particulars of all owners of the account, in Latin characters and in digits customarily used in the state of Israel.
34. For the purposes of Section 30–33:
- Identifying particulars of account owner:** for an individual—surname, first name, and ID number; for a corporation—name and registration number.
- Account particulars:** bank number, branch number, and account number.
