MANAGEMENT OF ANTI-MONEY LAUNDERING AND COUNTERING FINANCING OF TERRORISM RISKS

Contents

ONLY THE HEBREW VERSION IS BINDING

Chapter A: General

Introduction

1. Money laundering and the financing of terrorism (hereinafter: ML/FT), as activities in which money is transferred mainly for concealing or distorting their source, are perpetrated via the banking system, among other vehicles. Accordingly, banking corporations are at the forefront of the struggle to prevent them. Apart from the debasement of values against which relevant legislation provides a defense, the exploitation of a banking corporation for ML/FT 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. Accordingly, boards of directors and senior management must have in place policies and procedures for management of ML/FT risks, and must monitor their implementation, as inseparable parts of banking activity.
2. A risk-based approach contributes to the effectiveness of resource allocation for combating ML/FT, and to the implementation of risk-based measures in all Financial Action Task Force (FATF) recommendations.

   The main principle in this approach is that once a customer is classified as high-risk, a banking corporation must take more enhanced measures to manage and mitigate this risk. In assessing the risk, the banking corporation should take into account all of relevant risk factors before determining the overall level of risk and the measures that are needed to mitigate it.
3. The AML/CFT (anti-money laundering and countering the financing of terrorism) Officer, defined in Section 14 below, and his/her subordinates are part of a banking corporation's compliance function as defined in Proper Conduct of Banking Business Directive 308—"Compliance and the Compliance Function in a Banking Corporation" (hereinafter, Directive 308), and are integral parts of the second line of defense in a banking corporation's risk-management governance. This approach is consistent with the three lines of defense specified in Section 4 of Proper Conduct

of Banking Business Directive 310, "Risk Management" (hereinafter, Directive 310).

4. Importantly, nothing in the contents of this Directive shall be construed as a basis for denying banking services to economically or socially disadvantaged groups solely against this background.

Applicability

5. (a) This Directive shall apply to banking corporations and those corporations specified in Sections 11(a)(2) and 11(b) of the Banking (Licensing) Law, 5741-1981 (hereinafter, 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 banking corporation outside Israel, the provisions of Sections 42, 44, and 72–74 of this Directive shall not apply.

Definitions

6. All terms in this Directive shall be construed as set forth in the Prohibition of Money Laundering (Banking Corporations' Requirement regarding Identification, Reporting, and Record-Keeping) Order, 5761–2001 (hereinafter, the Order). Additionally, in this Directive:

"Politically Exposed Person (PEP)"	A foreign or domestic public figure or a senior officer in an international organization;
"Foreign Politically Exposed Person (FPEP)"	An individual who holds a senior public position outside of Israel;
"Domestic Politically Exposed Person (DPEP)"	An individual who holds a senior public position in Israel;

"Senior officer in an international organization"	A person who serves as a member of the senior management of an international organization, e.g., chief officer, deputy chief officer, member of the board of directors, or any other position of said type even if differently titled;
"Senior public position"	Including head of state, president of state, mayor, judge, member of Knesset or parliament, member of government, member of the management of a central bank, ambassador, senior member of a political party, high-ranking military or police officer, senior official of a state owned corporation and any official of said kind, even if differently titled;
"The Law"	The Prevention of Money Laundering Law, 5760-2000;
"AML/CFT Officer"	The person in charge of assuring a banking corporation's compliance with its AML/CFT obligations, appointed as specified in 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;
"Senior executive"	An executive officer in a banking corporation of a sufficiently high status who is familiar with the bank's AML/CFT policies and procedures.
"Acquirer"	As defined in Section 36i of the Banking (Licensing) Law, 5741-1981.

Chapter B: Corporate Governance

Board of directors

7. Within the framework of compliance-risk management as defined in Directive 308, the board of directors shall also oversee the management of ML/FT risks. In this context, the board of directors shall:
   (a) approve an AML/CFT policy as specified in Sections 10–11 below, in consideration of the banking corporation's risk assessment as set forth in Chapter C below.
   (b) specify ways in which staff shall be advised of the essence of said AML/CFT policy and the importance that the board of directors attributes to it.
   (c) ascertain that AML/CFT issues are dealt with effectively and promptly by senior management, with assistance from the AML/CFT Officer and other functions.
   (d) assess, at least once annually, the effectiveness of ML/FT-risk management at the banking corporation.
   (e) determine the type, content, and frequency of reports that it shall receive in regard to AML/CFT matters.
   (f) meet with the AML/CFT Officer alone, at least once per year, to help the board of directors carry out assessment of the effectiveness of ML/FT risk management at the banking corporation. Said meeting may also take place with one of the board of directors committees, as set forth in Section 35(e)(3) of Proper Conduct of Banking Business Directive 301, "Board of Directors."

Senior management

8. Senior management shall be responsible for effective management of ML/FT risks. In the discharge of its duties, it shall:
   (a) formulate a written AML/CFT policy that includes the basic principles by which management and staff shall act as specified in Sections 9–10 below.
   (b) establish procedures for implementation of the policy approved by the board of directors in order to prevent deliberate or inadvertent abuse of the banking

corporation by various entities. Said procedures shall include reference to the matters regulated by this Directive.

(c) assure the allocation of adequate resources to the AML/CFT Officer, including human resources, so that banking corporation's objectives may be attained.

(d) identify and assess, at least once annually, ML/FT risks that the banking corporation faces, as set forth in Section 23(b) below, and draft plans for managing and mitigating said risks.

(e) report to the board of directors or to one of its committees (Risk Management or Audit), at least once annually, about ML/FT risk at the banking corporation, in a manner that will help the board of directors to conduct an informed assessment of the extent of effectiveness of which the banking corporation's manages its ML/FT risks.

(f) immediately advise the board of directors or one of its committees (Risk Management or Audit) of material AML/CFT compliance failures such as those that pose a meaningful risk and may lead to the imposition of sanctions by legal instances or regulatory authorities, financial loss, or harm to reputation.

AML/CFT policy

9. (a) AML/CFT policy shall specify the way the banking corporation shall deploy in order to implement this Directive, including main processes in which ML/FT risks will be detected and managed at all corporate levels.

(b) Said policy shall be established on a group basis, *mutatis mutandis* as warranted by relevant legislation, regulation, and risk characteristics. Said group-level policy shall bear in mind that customers classified as belonging to one group may pose different risks in different jurisdictions.

10. The policy, and the procedures established based on said policy, shall cover the following issues, among others:

(a) provision of service to customers, including a know your customer procedure when an account is opened (customer acceptance policy) or when services are provided to a party carrying out a transaction in an account in which s/he is not

recorded as the owner or as an authorized signatory and while executing a significant transaction in the account in relation to his/her ongoing activity;

(b) classification of high risk customer groups;

(c) different know your customer rules for different types of customers;

(d) monitoring of account activity and heightened monitoring of high-risk customers;

(e) regular control of accounts and control of customer activity by means other than an account, in various ways (e.g., use of external public or private databases) commensurate with the level of exposure to risk;

(f) definition of the AML/CFT Officer's authorities and responsibilities, as specified in Sections 14–18 below;

(g) relations between the AML/CFT Officer and other functions that constitute the second line of defense and between the AML/CFT Officer and the Internal Audit function, as specified in Section 4(b) of Directive 310;

(h) use of new technologies, products, or services;

(i) types, formats, and frequency of reports that the AML/CFT Officer shall present to the management and to the board of directors of the banking corporation;

(j) cases in which the banking corporation shall take measures in regard to a customer's account as part of its risk-management activity, including restricting activity, prohibiting a specific transaction, and even closing the account;

(k) the bank's ability to scan and detect transactions that may be associated with FT and proliferation and the use of lists of organizations and of designated terror activists (e.g., those of the UN Security Council Sanctions Committee [UNSCR] and the US Department of the Treasury's Office of Foreign Assets Control—OFAC);

(l) executing transfers of money whose source or destination bank accounts appear on websites, ostensibly serving for illegal gaming activities and are included in the list published on the website of the Competent Authority;

(m) establishing business relations with or executing transactions for customers vis-à-vis designated parties that appear on international lists, as published by the

Sanctions Department at the Ministry of Finance, for assisting Iran in its nuclear program and programs related thereto;

(n) establishing business relations with or executing transactions for customers vis-à-vis elements declared by the UN Security Council Sanctions Committee, as shall be published on the Ministry of Foreign Affairs web site;

(o) customers' cross-border activities, with emphasis on tax obligations outside the country in which the account was opened, as detailed in Appendix B of this Directive;

(p) for a banking corporation that is an acquirer, a know your customer process for formation of business relations by an acquirer with an aggregator, taking account of the following factors at least: merchants' field of activity, the aggregator's expected extent of acquiring[1], and the aggregator's being under AML/CFT supervision, as specified in Sections 76–80 below.

(q) restrictions on the extent of issuing and acquiring activity of a banking corporation abroad, particularly in countries where the company does not have an incorporated and supervised presence, and also on relations with businesses that are active in risk-intensive industries or executing transactions in these industries via payment cards that it issued, as specified in Sections 84–87 below.

11. The policy document shall be reviewed at least once annually and updated in view of developments and changes in the external activity environment and the banking corporation's strategy, product line, activities, and systems.

12. A banking corporation shall act to anchor in its policy document the principle by which, in cases where concern about ML/FT arises or in a case where the customer or activity in the account is identified as being high risk, the banking corporation will be required to conduct a know your customer process irrespective of alternative identification procedures, other reliefs, or other exemptions set forth in the Directive, the Order, or any other regulation.

[1] "Acquring" in this Directive refers to activity termed "clearing" in the Debit Cards Law, 5746-1986.

Business units

13. A banking corporation shall specify, in its policies and procedures, the measures that business units on the first line of defense shall invoke, including setting controls and training staff so that the first line of defense will be equipped to implement the banking corporation's AML/CFT policy.

AML/CFT Officer

14. The AML/CFT Officer and his/her subordinates are part of the compliance function; accordingly, all rules that apply to said function, as specified in Directive 308, shall apply to him/her, including the following:
    (a) The AML/CFT Officer shall have a senior formal status at the banking corporation. He/she shall have credentials, knowledge, and experience befitting his/her duties and responsibilities.
    (b) In accordance with the contents of Section 33(a) of Directive 308, the Chief Compliance Officer shall also be the AML/CFT Officer. However, in the event that a Chief Compliance Officer is a member of the banking corporation's management, the AML/CFT Officer may be directly subordinate to him/her.
    (c) The AML/CFT Officer and his/her staff shall have unrestricted access to all customer identification records and information as well as additional know your customer documents, transaction documents, and any other relevant information.
    (d) The AML/CFT Officer of the parent company shall enjoy access to relevant information for the enforcement of group-level AML/CFT policies and procedures.
    (e) The AML/CFT Officer of the parent company shall ascertain that subsidiaries and branches have the tools to apply the group's AML/CFT policy; for this purpose, relevant staff members shall receive ongoing training.
    (f) The AML/CFT Officer of the parent company shall asssure the employment of staff that has relevant knowledge and experience in jurisdictions where subsidiaries and branches operate.

15. The AML/CFT Officer of the parent company shall assure the implementation of the banking corporation's AML/CFT policies and procedures at the group level, including ascertaining the effectiveness of central know your customer policy and requirements for information-sharing with other members of the group.
16. The AML/CFT Officer of the parent company shall make sure that relevant subsidiaries of the banking corporation, in Israel and abroad, are applying the group-level policy and have a professionally competent AML/CFT Officer.
17. The AML/CFT Officer shall present the management and board of directors of the banking corporation, directly, with an annual assessment report on the implementation of the banking corporation's policy, with reference to assimilating requirements flowing from statutes, regulations, and directives into its procedures, and on the banking corporation's risks and exposures as a whole.
18. (a) The AML/CFT Officer may discharge his/her duties under the Law, the Order, and the provisions of this Directive via a person whom he/she authorizes in writing for this purpose, and shall keep documentation in regard thereto.
    (b) Even if the AML/CFT Officer authorizes an employee at the banking corporation as set forth in Section (a), responsibility shall remain his/hers.
    (c) The AML/CFT officer of the parent bank shall review such risks, itemized by areas of activity, as are reported by subsidiaries and branches and, where necessary, shall assess the group-level risk posed by a given customer or group of customers; the provisions of this Section shall not derogate from the privacy rules that apply to the banking corporation's activity.
    (d) AML/CFT officers at subsidiaries and branches in countries other than Israel shall be professionally subordinate to the parent corporation's AML/CFT officer and not to the manager of the subsidiary or branch abroad.

Relations with Internal Audit

19. The AML/CFT Officer and his/her subordinates are part of the second line of defense; accordingly, they are liable to periodic independent audits by the Internal Audit function, which constitutes the third line of defense; said function shall advise

the AML/CFT Officer of audit findings that are relevant to the discharge of his/her obligations and shall monitor that identified deficiencies are corrected.

20. The Internal Audit function shall allocate adequate resources for its review of AML/CFT compliance at the banking corporation and its subsidiaries in Israel and abroad, including allocation of staff that has the knowledge and expertise to conduct internal audits in these areas; its inspections (including sample inspections) shall include policies, procedures, and controls.
21. In accordance with the provisions of Section 10(g) *supra,* it shall be the banking corporation's policy that the interal audit should address itself to the following:
    (a) the adequacy of AML/CFT policy in coping with risks detected;
    (b) the effectiveness of banking-corporation staff in implementing policies and procedures;
    (c) the effectiveness of oversight to assure compliance controls,including parameters of criteria for automatic alerts;
    (d) the effectiveness of training activities for relevant staff.
22. The Internal Audit function shall make sure that the audit scope, frequency, and methodology are determined on the basis of a risk-based approach. It shall also conduct periodic dedicated audits in this matter, so as to cover the various areas of banking corporation activity over time.

Chapter C: Risk Assessment

23. (a) A banking corporation shall conduct a comprehensive risk assessment, in which ML/FT risks that it faces will be identified and analyzed. Said risk assessment shall be the basis for the implementation of a risk-based approach by the banking corporation and, *inter alia*, will help assure appropriate resource allocation for the mitigation of identified risks.

    (b) A banking corporation shall review the risk assessment at least once annually and whenever circumstances change or new threats emerge, and shall update the risk assessment accordingly.

    (c) A banking corporation shall communicate the risk assessment to relevant staff in a focused and dedicated manner.

24. In conducting the risk assessment, a banking corporation shall consider a range of factors that are relevant to its activity, including:

    (a) the nature, scale, diversity, and complexity of its business and the services that it renders;

    (b) its target markets;

    (c) the number of customers already identified as high-risk;

    (d) the countries or territories to which it is exposed, either directly or via its customers' activity, with emphasis on high risk countries with high levels of organized crime or corruption, and/or countries with deficient AML/CFT controls as indicated by FATF publications;

    (e) its distribution channels, including the extent of its direct contact with customers and its reliance on technology;

    (f) findings of Internal Audit and audit reports of the Supervisor of Banks;

    (g) volume and size of transactions in view of the banking corporation's ordinary activity and customer profile.

25. A banking corporation shall draft said risk assessment on the basis of inforrmation that it shall collect from both internal and external sources, such as:
    (a) its business-activity and customer-relations managers;
    (b) relevant reports from the internal-audit function;
    (c) national risk assessments produced in accordance with relevant FATF recommendations for group or banking corporation activity;
    (d) lists of inter-governmental organizations and of national governments;
    (e) evaluation and progress reports by FATF or associated bodies as well as typologies published by them.
26. A banking corporation shall monitor ML/FT threats arising from the development of new products and business practices, including new delivery channels as specified in Section 16 of Directive 310, and from use of new and developing technologies for both new and pre-existing products, while taking steps to avoid such threats.

    Said risk assessment shall take place prior to the launch of said new or developing product, practice, or technology, and the banking corporation shall take appropriate measures to manage and mitigate said risks.

Chapter D: Risk Mitigation

Know your customer

27. The risk-mitigation policies, procedures, measures, and controls specified in this Directive shall be consistent with the banking corporation's risk assessment.

Risk factors

28. When establishing know your customer policies and procedures, a banking corporation shall bear in mind the following factors among others:

Risk factors—customers

(a) opening of an account is conducted under irregular circumstances, e.g., absence of linkage between the customer and the location of the banking corporation's branch;

(b) a non-resident customer who has no linkage to Israel;

(c) corporations or entities that were established under other legal arrangements and serve as asset-holding vehicles;

(d) a company in which a large portion of capital, or of the capital of its controlling company, is composed of bearer shares or held by a trustee, be this the customer, the beneficiary, or the holder of controlling interest;

(e) a cash-intensive business;

(f) a corporate structure that is exceptionally complex relative to the nature of its activity;

(g) a customer who is able to influence procurement decisions involving sizable sums of money;

(h) a customer who is active in fields known as being at high risk of involvement in corruption;

Risk factors—countries and territories

(i) high-risk countries;

(j) countries subject to sanctions, embargos, or measures of similar nature imposed by entities such as the United Nations;

(k) countries identified by credible sources as having significant levels of corruption or criminal activity;

(l) countries or terrritories identified by credible sources as providing funding or support for terrorism activity or that have designated terrorist organizations operating within their country.

Risk factors—products, services, and delivery channels

(m) private banking;

(n) payments or transfers from third parties that are unknown to the banking corporation or without linkage to the customer;

(o) anonymous transactions, including cash transactions;

(p) activity in an online account as defined and specified in Proper Conduct of Banking Business Directive 367, "E-Banking",

Risk variables

29. A banking corporation shall assess, by means of a structured and computerized Know Your Customer questionnaire, the level of AML/CFT risk that its activity with the customer presents to it, on the basis, among other things, of the risk variables specified below, weighted by risk factors:

(a) the purpose of opening the account, the circumstances surrounding the opening of the account, and the intended activity in the account, including the location of activity in consideration of the extent of regularity or duration of relations with the customer;

(b) the customer's line of business;

(c) the scale of assets and expected activity in the account;

(d) whether the customer, the beneficiary, or the holder of controlling interest is a Politically Exposed Person or a relative thereof, as defined in Section 63 below;

(e) *for a business account*—familiarity with the business, profile of customers and vendors, and an inquiry into the scale of intended business activity in the account;

(f) *for a corporate account*—familiarity with the control structure of the corporation by means of documents (e.g., articles of incorporation, shareholders' agreements, co-operation agreements) and with the names of the corporation's senior executives;

(g) inquiry into whether a banking corporation denied service to the customer for reasons related to AML/CFT.

High-risk activity

30. A banking corporation that, while conducting a know your customer process, identifies the customer or activity in the account as of high risk shall take one or more of the following actions:

(a) obtain additional information on the customer from publicly accessible databases or sources such as the Internet and updating more frequently the identification data of the customer or the beneficial owner;

(b) inquire into the source of the customer's wealth and the source of the funds that are to be deposited in the account;

(c) obtain information, explanations, and also, where necessary, written documentation in support of said explanations for transactions executed, or intended to be executed, in the account;

(d) Enhanced monitoring of the activity in the account by increasing the number and timing of controls applied, and defining patterns of transactions that entail further examination, as specified in Section 33;

(e) inquire into accounts that are linked to the customer's account;

(f) obtain authorization from a senior executive for opening or continued management of the account, including execution of significant transactions.

Monitoring of customer activity

31. A banking corporation shall monitor customer activity to determine whether it is consistent with the banking corporation's assessment of activity in the account and its familiarity with the customer, its business activity, and its risk profile, as formulated on the basis of the computerized questionnaire referenced in Section 29 *supra.*

32. A banking corporation shall have in place a computerized system to detect irregular activity in all of its customers' accounts and irregular activity in transactions that are not recorded in a customer account. This may be accomplished by setting limits on certain types of accounts. The banking corporation shall examine more intensively whether complex or unusually structured transactions are logical in economic or business terms.

    Unusual transactions include, *inter alia*, transactions lacking economic or business logic, complex transactions, sizeable transactions, and particularly large cash deposits in amounts that are not consistent with the customer's expected activity in the account.

33. Pursuant to the contents of Section 30(d) *supra,* a banking corporation shall maintain an organized control system and monitor high-risk customers' accounts by applying a special array of indicators for these accounts, bearing in mind, among other factors, the customer's background, the country of origin of the funds, and the types of transactions made.

34. A banking corporation shall operate an information system that will provide the AML/CFT Officer with readily available information for the analysis and efficient surveillance of high-risk customer accounts. Such information shall include unusual transactions executed via the customer's account and information about the relationship between the banking corporation and the customer over time. It shall also include reports on accounts for which documents are missing.

Record keeping

35. (a) A banking corporation shall establish procedures for the retention of information needed for the authentication of a customer's identity and type of business, with reference to the source of information, duration of retention, type of customer (individual, corporation, etc.), and expected scale of activity in the account. Said information shall be retained in a manner that will allow it to be efficiently retrieved and readily available.

(b) Said documents shall enable the banking corporation to reconstruct even individual transactions so that, where necessary, the information can provide evidence for prosecution of criminal activity.

(c) The retained documents shall also include account statements and business correspondence, e.g., inquiries to establish the background and purpose of complex, unusually large transactions.

(d) Said information shall be retained as set forth in Sections 7 and 14(b) of the Order, as the case may be.

36. (a) A banking corporation shall carry out reviews to ensure the existence of appropriate and up-to-date information and shall carry out heightened reviews of high-risk customers.

(b) Said reviews shall be carried out at times and upon the occurrence of events that the banking corporation specifies in its procedures, e.g., when a significant transaction is about to take place, when standards relating to requisite customer documents change, or when the way the account is managed changes significantly.

(c) If the banking corporation finds that meaningful information about a customer is lacking, it shall take steps to ensure that it obtains the relevant information as promptly as possible.

Training

37. (a) A banking corporation shall provide training in customer identification and due diligence, distinguishing among new staff, management staff, branch staff, staff

dealing with accepting new customers, and compliance-function staff, and shall advise staff of the procedures set forth.

(b) Said training shall be tailored to the relevant staff member or group of staff members in order to ensure that each possesses the knowledge and information to implement the banking corporation's policies and procedures effectively.

(c) Said training shall take place regularly in order to ensure that staff is equipped with up-to-date information including that relating to the latest techniques, methods, and trends. In said training, special attention shall be called to all directives pertaining to AML/CFT and, particularly, to requirements associated with reporting unusual transactions. A banking corporation shall take such actions as are necessary to assimilate the knowledge.

38. A banking corporation shall have procedures in place that assure high standards, including integrity, in hiring new staff commensurate with the nature of the position. For the purpose of this part of the Directive, "**staff**" shall include staff employed by personnel companies.

Reporting to Competent Authority

39. If a banking corporation detects irregular activity in an account, either pursuant to an alert from the computerized system referenced in Section 32 *supra* or in any other way, it shall perform the following:

(a) check the background and purpose of the irregular activity in the account and examine whether it constitutes activity that requires reportage under Section 9 of the Order;

(b) findings of said check shall be documented in writing and shall be available to the supervisory authorities and the auditors for a period no shorter than seven years from the date on which the decision on whether to report is made.

40. (a) A banking corporation shall set a detailed procedure that defines the internal channels of reportage on unusual transactions under Section 9 of the Order. Said procedure shall include full documentation of the decision-making process

from first detection to the decision on whether to report to the Competent Authority.

(b) Reporting an unusual transaction under Section 9 of the Order shall take place as promptly as the circumstances allow. 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 the delay.

(c) A banking corporation shall retain documentation of reportage to the Competent Authority for a period no shorter than seven years from the date of said report.

Customer identification

41. A banking corporation shall record the name and ID number of any person who makes a transaction in an account in which s/he is not recorded as the owner or an authorized signatory. For the purpose of this Section, a banking corporation may content itself with particulars given by the transactor.

    In this Section, the word **"transaction"** denotes a transaction in cash in a sum smaller than 10,000 New Israel Shekels or another transaction in a sum smaller than 50,000 New Israel Shekels.

42. A banking corporation shall record the ID number of a public institution as assigned to it in accordance with the "Entities without Statutory Registrar" register, managed by SHAAM (the computerized processing system) of the Israel Tax Authority.

43. A banking corporation shall assign a standard and one to one value ID number that it shall use to represent:

    (a) a recognized entity and a corporation established under a foreign statute (e.g., a central bank, etc.);

    (b) a public institution that is not registered with SHAAM and was not assigned an ID number even after an inquiry with SHAAM was made.

44. A banking corporation shall launch identification proceedings that correspond to identification situations that take place under Paragraphs (1)–(4) of Subsection 6(a) of the Order.

45. If the account holder is a corporation, the banking corporation shall record the individual who controls the corporation as the holder of controlling interest; if the corporation is controlled by a chain of holdings, the banking corporation shall understand the entire chain up to the individual who holds controlling interest.

46. (a) A banking corporation shall take reasonable measures to detect electronic transfers of foreign origin, destined to Israel, that lack information about the parties thereto as required by Section 2(k) of the Order.

    (b) A banking corporation that receives an electronic transfer that originates from abroad at an amount exceeding NIS 5,000, shall authenticate the identification details of the transfer recipient, to the extent that they were not previously authenticated by it, and shall keep the transfer documents,.

    (c) A banking corporation that receives an instruction to carry out an electronic transfer to abroad, shall authenticate the identifying details of the service recipient to the extent that these were not authenticated by it in the past, except in cases where the amount of the transfer does not exceed NIS 5,000 and does not raise suspicion of money laundering or terrorism financing.

    (d) An intermediating banking corporation (correspondent) that receives an electronic transfer originating from abroad, where the destination is another banking corporation on behalf of its customer, shall keep the transfer document for a period of at least 7 years, if it was unable, for technical reasons, to transfer the transfer documentation to the other banking corporation.

47. (a) A banking corporation that receives a transfer from abroad shall have risk-based procedures in place to determine whether it should be accepted, rejected, or suspended, as set forth in Section 46(a) *supra*, because as a rule a transfer lacking information about its parties should not be accepted. This obligation shall apply both to a banking corporation managing the beneficiary's account and to an intermediating banking corporation through which the the transfer was executed.

(b) Said procedures shall relate, among other things, to the type of information missing, the country of origin of the transfer, the sum of the transfer, the recipient's identity, and the essence of the payment.

(c) Said procedures shall relate to cases in which a request for this information is presented to the bank that initiated the transfer or to an intermediary bank.

48. (a) A banking corporation shall not execute a customer's instruction to make an electronic transfer in Israel unless the particulars of the transferor and the transferee, as specified in Section 2(k) of the Order, appear.

(a1) A banking corporation that receives an instruction from a customer in Israel to carry out an electronic transfer, shall verify that it can submit the items noted in Subsection (a), to enforcement authorities, immediately, if required.

(b) A banking corporation shall not accept an electronic transfer from abroad unless it includes the IBAN details of the transferee's account except in the presence of circumstances that the bank has specified in its procedures.

48a. A banking corporation shall not execute several electronic transfers in one batch to outside of Israel, for the same transferor without having the particulars of the transferor and transferee as determined in Section 2(k) of the Order for each transfer in the batch. With regard to this subsection, "batch"—several transfers for the same transferor to various transferees, that are transferred in one file.

49. When an account is opened online, the provisions set forth in Chapter C of Proper Conduct of Banking Business Directive 367, "E-Banking," shall apply.

Reasonable refusal

50. The presence of one or more of the following conditions shall be deemed reasonable grounds for refusing to open and manage an account, including the carrying out of certain transactions in the account, and for providing service to a transactor who is not recorded as the owner or authorized signatory of an account for the purposes of the Banking (Service to the Customer) Law, 5741-1981:

(a) customer failure to share necessary details to satisfy the provisions of the Order, this Directive, and policy and procedures of the banking corporation as set forth on the basis thereof;

(b) reasonable grounds for concern that a transaction is associated with ML/FT.

(c) execution of the know your customer process will lead to a violation of the prohibition established in Section 12 of the Order. Non-execution of the transaction, including non-completion of the know your customer process or not opening an account or ending the relationship with the customer, do not obviate the banking corporation's obligation to examine the need for reporting to the authorized authority on irregular activity in accordance with Section 9 of the Order.

Non-performance of a transaction or even termination of relations with the customer shall not absolve the banking corporation of its duty to consider the need to report an unusual transaction to the Competent Authority as set forth in Section 9 of the Order.

Chapter E. Risk Activity

Numbered accounts

51. A banking corporation shall not open numbered accounts (accounts in which the banking corporation knows the owner's identity but substitutes numbers or aliases for identifying particulars in its records).
52. A banking corporation shall open neither anonymous accounts nor accounts in fictitious names.

Third-party accounts

53. A banking corporation shall take necessary measures to understand the relationship between entities that are associated with accounts managed by a trustee (e.g., legal guardian, liquidator, executor, receiver, attorney, or accountant etc.).
54. A banking corporation shall record the identifying particulars of persons who establish and, if any, serve as protectors of a trusteeship and shall take reasonable measures, relative to the extent of ML/FT risk, to verify their identity.
55. In opening a trustee account with multiple beneficiaries who can be profiled, the banking corporation may settle for a general recording of the beneficiaries, provided the account owner undertakes to disclose the beneficiaries' identity when they are to be paid, when their rights under the trusteeship are to be exercised, or in any case that requires it.
56. A banking corporation shall neither open nor manage an account for a customer who acts on behalf of a third party and does not share requisite information about said third party.
57. The provisions of Sections 53–56 *supra* shall also apply to similar legal arrangements that are not trusteeships.

Politically Exposed Persons (PEPs)

58. (a) When opening an account for a new customer and when updating know your customer particulars for an existing customer, a banking corporation shall check whether the customer, the beneficiary, or the holder of controlling interest is a PEP. Said examination shall take place, among other steps, by direct inquiry with the customer and also—where necessary, following a risk-based approach, and to the extent possible—by searching for publicly available information online and in a commercial electronic database.

(b) If it is found in the course of relations that the customer, the beneficiary, or the holder of controlling interest is a PEP, the banking corporation shall act as required when opening an account for a PEP.

59. Before opening an account for a PEP and in the course of the business relationship, a banking corporation shall take steps to identify the source of funds that are expected to be deposited in the account and the source of the PEP's wealth. The factors that the banking corporation shall bear in mind shall include:

(a) classification of the country in which the customer is considered a PEP, with reference to the quality of its AML/CFT regime, and reports on corruption such as those published by the United Nations;

(b) unexplained sources of wealth or income;

(c) expectations of receipts of large sums from government entities or state-owned entities;

(d) a source of wealth that is described as commission earned from government contracts;

(e) use of government accounts as a source of funds for a transaction.

60. The decision to open an account for a foreign PEP or a senior officer in an international organization shall be taken by a senior executive.

61. (a) An account of a customer, a beneficiary, or a holder of controlling interest who is a foreign PEP or a senior officer in an international organization shall be defined as an account of a high-risk customer and, accordingly, the banking corporation shall take the measures specified in Section 30 *supra.*

(b) If a banking corporation finds that a domestic PEP is a "high-risk customer" on the basis of information obtained in the course of the know your customer process set forth in Sections 28–30, and in consideration of the level of seniority and access to public funds, the banking corporation shall take all measures that are specified in this part of the Directive in regard to business relations with a foreign PEP, in regard to business relations with a domestic PEP as well.

62. A banking corporation shall also act in the manner set forth in Sections 58–61 in regard to an individual who **held** a senior public position or was a member of senior official of an international organization, using a risk-based approach in accordance with the following risk variables: rank of his/her post, time passed since he/she concluded his/her term of service, and the relationship between said position and his/her current vocation.

63. For the purposes of Sections 58–62, management of an account of a relative of a PEP shall be considered equivalent to management of an account of a PEP.

A **"relative"** is one of the following:

(1) a family member—including spouses, parents, siblings, and children;

(2) a corporation controlled by a PEP;

(3) a close associate—an individual who is known to be a co-holder of controlling interest in a corporation or a trusteeship, a person who has business relations with a PEP, or an individual who is the sole holder of controlling interest in a corporation or a trusteeship that is known to have been established, de facto, for the benefit of a PEP.

Correspondent account

64. A banking corporation that manages correspondent accounts shall conduct an assessment of ML/FT risks associated with the management of said accounts and, in accordance with said assessment, shall apply the appropriate know your customer measures specified in Sections 65–66 below.

Know your customer

65. When opening an account, as well as on an ongoing basis, a banking corporation that manages correspondent accounts shall collect sufficient information from questionnaires and, where necessary, from publicly available sources, to know and understand the essence of the business dealings of the banks with which it maintains a correspondent account ("respondents") in consideration of the following factors:
    (a) information about the management of, and holders of controlling interest in, the respondent bank (particularly if PEPs are involved), its major business activity, its place of incorporation and business dealings, and its customers and their domiciles;
    (b) the reputation of the respondent bank, including whether it has been subjected to an AML/CFT-related investigation or other regulatory action;
    (c) the respondent bank's AML/CFT policy and its monitoring and control procedures, including description of its know your customer procedures;
    (d) the purpose of the account being opened and the services that the respondent bank shall receive;
    (e) the condition and quality of supervision and regulation in the country where the respondent bank is located, with emphasis on its AML/CFT regime, including its being at higher risk, and also, in the case of a banking group, the state of supervision and regulation in the countries where its branches and subsidiaries are located;
    (f) the ability to obtain identifying particulars of third parties who will be entitled to use the correspondent accounts;
    (g) the possibility that other respondent banks that maintain correspondent relations with the respondent bank will be using the correspondent account.

66. (a) A banking corporation shall not content itself only with obtaining documents from the respondent bank; but, it will meet, to the extent necessary, with the bank's management, its compliance officer, and relevant regulators in the country of the respondent bank's activity, subject to their consent.

(b) To gather the requisite information, a banking corporation shall also make use of evaluation reports from the FATF and FSRB (FATF-Style Regional Bodies) and accessible relevant information published by authorities in the respondent bank's country.

67. Without derogating from the provisions of Section 65 *supra,* when a correspondent account is opened, the following shall also apply:
    (a) A banking corporation shall neither open nor manage a correspondent account for a financial institution that is not under AML/CFT supervision.
    (b) A banking corporation shall neither open nor manage a correspondent account with a bank registered in a jurisdiction where it does not maintain 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.
    (c) Decisions on opening new correspondent accounts and continuing to manage them shall be made by a senior executive.

Ongoing monitoring

68. A banking corporation that manages a correspondent account shall have in place appropriate policies and procedures to detect the following:
    (a) activity inconsistent with the purpose of the services provided to the respondent bank;
    (b) activity contrary to commitments that were concluded between the correspondent bank and the respondent bank.
69. Reportage on high-risk correspondent accounts and the manner of their monitoring shall be brought to the knowledge of senior management on an ongoing basis.
70. In cases where the banking corporation allows customers of a respondent bank to make transactions directly in a correspondent account, it shall monitor said activity commensurate with its specific risk; similarly, it shall make sure that the respondent bank conducts appropriate due diligence vis-à-vis these customers and is able to forward this information to the correspondent bank upon request.

Financial activity with banks operating in the Palestinian Authority areas

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

72. 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 Israel.

73. 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.

74. 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 Israel.

75. For the purposes of Sections 71–74:

Identifying particulars of account owner: for an individual—surname, first name, and ID number; and for a corporation—name and registration number.

Account particulars: bank number, branch number, and account number.

75a. (a) When making wage payments to Palestinian workers via bank transfers into accounts managed at banks in the Palestinian Authority, the banking corporation shall act in accordance with Supervisor's Circular of June 30, 2022, attached as Appendix D of this Directive.

(b) The provisions of Subsection (a) shall not apply when making wage payments to Palestinian workers employed by Israelis in Judea and Samaria; the Supervisor

of Banks may determine different Directives in this regard, under circumstances in which information on these workers can be verified.

Activity with Aggregators

76. In Sections 77–80:

"**Aggregator**"—a corporation that concentrates merchants' debits and credits carried out via payment cards, provided that the corporation has a license pursuant to the Control of Financial Services (Regulated financial services) Law, 5776-2016 or is a regulated financial entity that received a permit to continue operations and whose license request was not rejected.

"Merchant"—a business that engages in retail activity comprised of the sale of services or goods.

77. An acquirer shall not concentrate debits and credits for an aggregator until it receives a list of merchants with which the aggregator transacts, as well as an undertaking from the aggregator to update the acquirer regularly as to every merchant that is added to or deleted from the list of merchants in its possession.

78. An acquirer that provides an aggregator with acquiring services even in cases where it has no direct acquiring agreement with the merchant may do so provided the annual extent of acquiring for an individual merchant does not exceed NIS 2,000,000.

Notwithstanding the above, to the extent that the reference is to an aggregator on whose activity as an aggregator an Order, under the Prohibition on Money Laundering Law, 5760-2000, and under the Combatting Terrorism Law, 5776-2016, is not imposed, the limit on the scope of annual acquiring for an individual merchant shall be a total of NIS 100,000.

In the cases noted above, an acquirer shall establish procedures for merchant due diligence—on the basis of the know your customer policy set forth in Section 11(q) *supra*—by means of the aggregator, provided that it has controls in place for the examination conducted by the aggregator.

79. An acquirer shall obtain from the aggregator details at the level of each transaction that a customer carries out with each merchant, including merchant's name, transaction sum, and transaction date.
80. The aggregator shall assure the acquirer that it is not acting on behalf of any other aggregator.
81. The AML/CFT Officer shall confirm every formation of business relations by an acquirer with an aggregator.

Transfers of Funds—High-Risk Countries

82. (a) A transfer of funds by means of a financial institution in a high-risk country, where the final destination is a financial institution in another high-risk country, for itself or for its customer, must be approved by the AML/CFT Officer.
    (b) A banking corporation shall maintain a computerized information system for transfers of funds to and from high-risk countries; said system shall provide the AML/CFT Officer with handy information on, among other things, customer name and account number, as is needed to detect and monitor these transactions efficiently and determine whether they are irregular.

Check depositing

83. A banking corporation shall establish, in its procedures, rules for handling the implicit risk of check depositing in the AML/CFT context, with reference to the following factors among others:
    (a) endorsed checks;
    (b) deposits of numerous checks, which are not consistent with the activity in the customer's account;
    (c) checks drawn on foreign banks; in such cases, before the clearing transaction takes place, the banking corporation shall ensure the existence of a linkage between the depositing of the check and the performance of a transaction with a banking corporation in Israel.

Management of risks involving payment card[2] transactions in risk-intensive industries

84. In Sections 85–87:

"**Risk-intensive industries"**—gambling, pornography, and the sale of a "curative drug", "toxin", "medical toxin", and "preparation" in the sense of these terms in the Pharmacists Order [Revised Version], 5741-1981, and any other area of activity that the board of directors defines as risk-intensive;

"Missing-document transaction"—a transaction between a customer and a vendor in which no payment card is presented upon the execution of the transaction; for this purpose, "presentation of card" is as defined in Section 12(1)(b) of Directive 470.

85. An acquirer company shall not approve a missing-document transaction made by means of a payment card that it issued, whether said transaction was executed online or in any other way, if information in its possession gives it reason to be concerned that the charge was made for a "prohibited game," a "lottery," or "gambling" as these terms are defined in Section 12 of Chapter 8 of the Penal Law, 5737-1977 (hereinafter: "the Penal Law"), with the exception of activity permitted under the Penal Law, and, in addition, where there is concern that one of the following conditions relating to the transaction is present:
    (a) the service for which the charge using the payment card was made is illegal in the country where the service was provided;
    (b) payment for said transaction is to be charged by means of a payment card belonging to a customer who is an Israel resident or who is a nonresident staying in Israel.

86. An acquirer shall not execute an agreement for the acquiring of missing-document transactions, whether this be done online or in any other way, with customers (businesses) in Israel or abroad, unless according to the information in its possession the customer's area of activity does not constitute a violation of the law.

[2] "Payment card" refers to credit and debit cards. The term "payment card" in this Directive is termed "debit card" in the Order.

87. An acquirer shall not enter into a relationship with customers (businesses) outside Israel who are active in risk-intensive industries, such as that stated in Section 85 above, unless:

(a) At the time the agreement is executed, the company possesses a legal opinion stating that the customer's area of activity does not constitute a violation of the law, e.g., prurient advertising featuring the image of a minor, prohibited gambling, and prohibited marketing of "curative drugs," "toxins," "medical toxins," or "preparations". Said legal opinion shall refer to the law that applies to the parties to the transaction, in all their centers of activity, as follows:

(1) the vendor in the missing-document transaction (in this Section: the business);

(2) other players, such as brokers and aggregators, that provide the credit card company with service vis-à-vis the business.

(b) At the time the agreement was executed, the acquirer took the requisite measures to verify that the customer (the business) does not execute missing-document transactions with service recipients (customers of the business) whose country's laws prohibit them from executing such transactions. The acquirer shall apply the provisions of this Paragraph at least to service recipients from countries that are members of the Organization for Economic Cooperation and Development (OECD).

(c) An acquirer shall periodically monitor the compliance of the business with the requirements of this Section.

(d) An acquirer that enters into such an agreement shall install appropriate procedures to ensure its compliance with the requirements of this Section throughout the term of the agreement.

Payment Services Related to Customer Activity in Virtual Currency

87A. In Sections 87A(a)-(g):

"**Financial asset**" - As this term is defined in Section 11A of the Control of Financial Services (Regulated Financial Services) Law, 5776-2016;

"**Currency**" and "**Foreign Currency**" – as these terms are defined in Section 1 of the Bank of Israel Law, 5770-2010;

"**the AML Order**" – the Prohibition on Money Laundering (Identification, Reporting, and Record Keeping Requirements of Financial Asset Service Providers and Credit Service Providers to Prevent Money Laundering and Financing of Terrorism) Order, 5781-2021;

"**Virtual Currency**" and "**Virtual Currency Wallet Address**" – as these terms are defined in Section 1 of the AML Order;

"**Virtual Currency Service Provider**" – a financial asset service provider, as this term is defined in Section 1 of the AML Order;

"**Payment Services Related to Activity in Virtual Currency**" – a transfer of money from accounts of Virtual Currency Service Provider to accounts of customers of the banking corporation who are not Virtual Currency Service Providers;

"**Virtual Currency Pathway**" – The transactions performed in virtual currencies or in a virtual currency wallet address in which virtual currencies were placed throughout their holding period, with emphasis on the identities of the transferors and transferees, and conversion pathway of the virtual currency into currency or foreign currency, including transactions in currency or in foreign currency from the date of the virtual currency conversion to currency or foreign currency to the date of its deposit into an account in the banking corporation;

(a) The banking corporation will periodically carry out an AML/CFT risk assessment of transfers of money, the source or destination of which is related to virtual currencies.

(b) On the basis of said risk assessment, the banking corporation shall define a policy and procedures for payment services related to activity in virtual currency, which will reflect a risk-based approach that addresses the following parameters, among others: the type of virtual currency and degree of anonymity that it affords users; the type of virtual currency and

the scope of its use; the identity of the virtual currency service provider; and the customer's activity profile.

The policy and procedures will include the following principles and topics at minimum:

(1) A banking corporation will not refuse to provide payment services related to activity in virtual currencies only because the source of the activity is connected to virtual currencies, if the virtual currency service provider that is a party to virtual currency operations was granted a license by the Capital Market, Insurance, and Savings Authority to render a financial asset service in Israel with respect to virtual currency services.

(2) The banking corporation will define its mode of operations vis-à-vis virtual currency service providers operating in Israel under a permit to continue to engage in financial asset service provision issued by the Capital Market, Insurance, and Savings Authority and vis-à-vis virtual currency service providers that are incorporated outside Israel and received a license or are registered under the laws and regulation of the virtual currency service provider's country of incorporation. The mode of operations will be defined based on a risk-based approach that takes into account the following factors, among others: the Virtual Currency Service Provider's country of incorporation and the AMF/CFT rules and regulations requirements that apply to its operations, the Virtual Currency Service Provider's policy and procedures concerning AML/CFT risk management (to the extent that such policy and procedures are known to the banking corporation).

(3) The banking corporation will determine the Virtual Currency Pathways through which it will permit payment services related to activity in virtual currency, taking into account its assessment of the risks.

For example, risk-reducing pathways may be: virtual currency that is received directly from mining activity, where the specific virtual currency wallet address had no additional movements, or virtual currency that is acquired from and sold to the same virtual currency wallet address for a specific customer, where the specific virtual currency wallet address had no additional movements.

(4) If the annual scope of payment services related to activity in virtual currency exceeds NIS 100,000, the banking corporation must obtain information from the customer about the source of the funds used to purchase the virtual currency or used to finance the virtual currency mining activity, and information about the Virtual Currency Pathway.

(5) The banking corporation will define its policy on payment services related to customers' activities via a P2P platform that facilitates trading in and exchange of virtual currencies for currency or foreign currency without the platform's intervention or supervision, and will define controls that will be put into place when such services are rendered.

(c) The banking corporation will obtain information on the virtual currency pathway using a risk-based approach, and such information may be based on a no-impediment certificate by a licensed virtual currency service provider in Israel stating that there is no impediment that prevents the execution of the transaction, or a declaration by a customer or confirmation by an outside expert, to the satisfaction of the banking corportion, which supports and confirms the virtual currency pathway—to the extent that the above certificate or declaration is consistent with the banking corporation's risk assessment.

(d) The banking corporation will not render payment services related to activity in virtual currency when, based on the information it possesses, the virtual currency service provider is in violation of the law with

respect to the licensing or registration requirements in its country of incorporation.

(e) The banking corporation will publish on its website the key points of its policy on payment services related to activity in virtual currency. In addition, if the banking corporation identifies that the customer wishes to transfer funds from its account administered by the banking corporation to an account administered by a virtual currency service provider, the banking corporation will also inform the customer of its policy, including information on the conditions for transferring funds from the customer's account with the virtual currency service provider to the customer's account with the banking corporation. The disclosure will be made immediately after, and if possible before, customers' first request to withdraw funds from their account with the banking corporation to their account with a virtual currency service provider. Furthermore, the disclosure will be made in a manner that does not constitute the imposition of undue influence on the customer with respect to the virtual currency service provider.

(f) At least once every six months, the senior management and board of directors of the banking corporation will receive reports on the scope of activities involving virtual currencies, the focal points of risks entailed in such operations, and how these risks are being monitored.

(g) Following Section 5 of Proper Conduct of Banking Business No. 100 "Introduction to the Proper Conduct of Banking Business Directives File," a banking corporation that is not one of the five largest banking corporations may request exemptions from the requirements of this section from the Banking Supervision Department, after presenting a reasoned risk assessment.

Chapter F. Scope of Activity—Group Risk Management

88. (a) A banking corporation that operates internationally via subsidiaries or branches in certain given jurisdictions shall have a group AML/CFT policy in place. Said policy and procedures at subsidiaries or branches shall be consistent with those of the group but shall allow local requirements to be implemented.

(b) In cases where the requirements at the jurisdictions, with emphasis on high-risk countries where subsidiaries or branches operate, are different from the provisions of this Directive, the stricter of the provisions shall apply provided they do not contravene the provisions of local law.

(c) If the stricter provisions are found to contravene the provisions of law in the host country as set forth in Subsection (b), the banking corporation shall take additional measures to manage AML/CFT risks, such as installing supplemental controls at both the branch and the group levels and shall consider the continuation of activity in the country in question.

The banking corporation shall report said measures as part of its compulsory reportage to the Banking Supervision Department under Section 91.

89. (a) When conducting risk assessment, the banking corporation should understand, document and update the risks on an ongoing basis, commensurate with the level of risk in the group;

(b) In assessing customer risk in subsidiaries or branches abroad, the banking corporation shall identify all relevant risk factors such as geographical location and patterns of transaction activity and usage of the banking corporation products and services and establish criteria for identifying higher-risk customers.

90. (a) A banking corporation shall tailor its monitoring procedures to existing risks in the jurisdiction where its branch or subsidiary operates; said monitoring shall be complemented by a process of information-sharing with the parent company

and also, if necessary, with other subsidiaries and branches, in respect of accounts and activity that represent heightened risk.

(b) To achieve effective group monitoring and management of ML/FT risks, banking corporations in the group shall share information about their customers in every jurisdiction, provided the information exchange does not contravene the provisions of such laws, including privacy laws, that apply to its activity.

(c) Subsidiaries and branches shall share with the appropriate control and audit functions at the parent corporation information about high-risk customers and activities that are relevant for the implementation of group-level policies and procedures.

(d) A banking corporation's group-level policies and procedures shall include a description of the process required for identification, monitoring, and investigation of unusual circumstances and reporting irregular activity.

Chapter G: Reporting to the Banking Supervision Department

91. (a) A banking corporation shall immediately advise the Banking Supervision Department of special cases that it reported to the Competent Authority within the framework of the compulsory reportage and are material to the stability or good reputation of the banking corporation.

(b) A banking corporation shall immediately advise the Banking Supervision Department of any investigation with ML or FT implications that is under way against itself or against a corporation that it controls.

(c) A banking corporation shall advise the Banking Supervision Department of the number of reports forwarded to the Competent Authority, itemized by types of reports, as well as addtional quantitative data as specified in Reporting to Banking Supervision Directive 825—"Semiannual Report on Exposure to Compliance Risks."

(d) A banking corporation shall advise the Banking Supervision Department whenever a foreign company that it controls, a foreign company in which it is an interested party, or a branch of the banking corporation abroad is not operating in accordance with this Directive because the Directive clashes with local laws.

Appendix A.1

Arrangement Established by the Supervisor of Banks under Section 5(a)(8) of the Order

The provisions of Sections 2(b) and (d)(2) and 4(a) of the Order—pertaining to the recording of an account beneficiary shall not apply to a trustee account that is managed on behalf of a "transparent" Exchange-Traded Note that tracks the Tel Aviv Banks Index, in which the mechanism established for the exercise of voting rights, as stated in Section 4.1.2 of the outline—are approved by the Israel Securities Authority and the Bank of Israel with regard to the existence of the operational test established in the outline.

Appendix A.2

Arrangement Established by the Supervisor of Banks under Section 5(a)(8) of the Order

The provisions of Sections 2(b), 2(d)(2), and 4(a) of the Order, pertaining to the recording of a beneficiary in an account shall not apply to a trustee account of a company with a platform license pursuant to Section 44(m) of the Securities Law, 5728-1968, for its customers, in accordance with the provisions of Section 21(a) of the Securities (Trading Platform for its Own Account) Regulations, 5775-2014.

Appendix A.3

Arrangement Established by the Supervisor of Banks under Section 5(a)(8) of the Order

The provisions of Sections 2(b), 2(d)(2), and 4(a) of the Order, pertaining to the recording of a beneficiary in an account, shall not apply to accounts of entities that are holders of a license to extend credit or holders of a license to provide services in a financial asset or holders of a license to operate a credit intermediation system, as defined in Sections 11a and 25q of the Control of Financial Services (regulated financial services) Law, 5776-2016, respectively, that are managed on behalf of their customers,

and that a valid Order applies to their activity as holders of a license, pursuant to the Prohibition on Money Laundering Law, 5760-2000, and pursuant to the Combatting Terrorism Law, 5776-2016, provided that the sole activity in such accounts is carried out by force of said licenses.

Appendix A.4

Arrangement Established by the Supervisor of Banks under Section 5(b) of the Order

The provisions of Sections 2(c), 2(d)(3), and 4(b) of the Order, pertaining to the obligation to record a controlling interest, shall not apply to accounts of entities that are holders of a license to extend credit or holders of a license to provide services in a financial asset or holders of a license to operate a credit intermediation system, as defined in Sections 11a and 25q of the Control of Financial Services (regulated financial services) Law, 5776-2016, respectively, that are managed on behalf of their customers, and that a valid Order applies to their activity as holders of a license, pursuant to the Prohibition on Money Laundering Law, 5760-2000, and pursuant to the Combatting Terrorism Law, 5776-2016, provided that the sole activity in such accounts is carried out by force of said licenses.

Appendix B

Arrangement Established by the Supervisor of Banks
pursuant to Section 7a of the Order

Notwithstanding the provisions of Chapter 2 of the Prohibition on Money Laundering (The Banking Corporations' Requirement regarding Identification, Reporting, and Record-Keeping for the Prevention of Money Laundering and the Financing of Terrorism) Order, 5761-2011, when opening a "Bank account", a banking corporation shall record the identifying particulars regarding a "Parent" and an "Eligible child," as specified in Section 2(a)(1)–(4) of the Order, on the basis of a computerized record sent to it by the National Insurance Institute.

In this regard:

"Eligible child," in the sense of this term in Paragraph 5 of Chapter 4 of the National Insurance Law [Combined Version], 5755-1995; **"Bank account"** and **"Parent"**—as defined in the National Insurance (Long-Term Savings for Child) Regulations, 5776-2016.

Appendix B.1

The arrangement established by the Supervisor of Banks in accordance with Section 7a of the Order:

By the power of my authorization under Section 7a of the Prohibition on Money Laundering (The Banking Corporations' Requirements regarding Identification, Reporting, and Record-Keeping for the Prevention of Money Laundering and the Financing of Terrorism) Order, 5761–2001, I hereby establish the following:

1. When opening an account for a political asylum seeker in Israel or for a temporary beneficiary of nondistancing policy ("the customer"), the banking corporation is to list the identification details noted in Section 2(a) of the Order as follows:
   (a) The identification number shall be according to the number in appearing in the license by power of Section 2(a)(5) of the Entry into Israel Law, 5712-1952, (hereinafter, "the Entry into Israel law") in the "passport number" field or as it appears in the Class B/1 license issued by the Population and Immigration Authority;
   (b) The date of birth shall be according to the number appearing in the license by power of Section 2(a)(5) of the Entry into Israel Law, and in the absence of said license, as submitted by the customer;
   (c) Address and gender shall be as the customer submitted to the banking corporation; address shall be the customer's place of residence in Israel including the name of the city, as well as the street name, the house number, and zip code, if such data exist.

2. The banking corporation shall authenticate the customer's identification details as follows:
   (a) Based on a valid residence license by power of Section 2(a)(5) of the Entry into Israel Law, issued by the Population and Immigration Authority and that is renewed once per period or based on a valid Class B/1 license issued

by the Population and Immigration Authority; a photocopy of the license shall be kept at the banking corporation.

(b) To the extent that the customer was issued the 2 types of license noted in Subsection (a)—based on the two licenses, a copy of which shall be kept at the banking corporation.

(c) Authentication of the identification details shall only be made with regard to the identification details appearing in the licenses.

3. A banking corporation may examine the originality of the customer's residence license under the power of Section 2(a)(5) of the Entry into Israel Law, based on sample licenses that appear on the website of the Population and Immigration Authority[3], with an emphasis on additional signs.[4]

4. Opening the account shall be contingent on a written declaration by the customer that this is the customer's only account in Israel.

5. The banking corporation shall limit the possible amount of the balance in the account according to the decision of the AML Officer with regard to the AML/CFT risk and in accordance with the customer's scope of activity as declared when opening the account. The banking corporation is to establish controls regarding the deviation of the amount of the balance in the account from the maximum established, while using discretion by the AML Officer in approving the deviation, in accordance with circumstances. If a transaction was carried out that requires reporting in accordance with Section 8 of the Order, the AML Officer, in line with the extent of AML/CFT risk, will consider the need to examine the circumstances of the transaction.

[3] https://www.gov.il/he/Departments/General/types_of_visas_for_infilitrators

[4] Picture, watermark, signatures stamped on the license (at least 2, of which at least 1is stamped on the picture), light brown or red lines on the front of the license and white lines on the back of the license; the passport number that appears as a permanent number on the license (the license number changes and therefore is not used as a sign of being an original;

6. If the customer requested to carry out an activity as noted in Sections 2 (f) and (g) of the Order, the banking corporation shall record its details and authenticate them as required by the provisions of Sections 1 to 2 above; the banking corporation shall keep a photocopy of the licenses through which it authenticated the identification details.

7. To the extent that it arises, from surveys carried out by the banking corporation, as required under Section 36 of the Directive, that the expiration date of the customer's identification document has passed, or in other cases, it shall send the customer a warning of such. If the customer does not provide the banking corporation with a valid identification document within 60 days from the date the warning letter is sent, or in cases of presenting an unoriginal license, the banking corporation shall not carry out any action initiated by the customer in the customer's account, except for withdrawing the existing balance in the account, repaying debts, and closing the account.

In this arrangement:

"Political asylum seeker"—one who submitted a request for political asylum in Israel and holds a valid license by the power of Section 2(a)(5) of the Entry into Israel Law, 5712-1952, (hereinafter, "the Entry into Israel law").

"Temporary beneficiary of nondistancing policies"—one who belongs to a group eligible for temporary protection from distancing and received a license by the power of Section 2(a)(5) of the Entry into Israel Law or a B/1 work license granted by power of Section 2(a)(5) of the Entry into Israel Law.

Appendix B.2

The arrangement established by the Supervisor of Banks in accordance with Section 7a of the Order:

Notwithstanding the provisions of Chapter B of the Order, when a banking corporation provides payment services for a service recipient, the banking corporation may act as follows:

1. To record the identification particulars detailed in Section 2(a) of the Order regarding the service recipient.
2. To record the particulars of the payment account and of the means of payment (to the extent that the means of payment is used in providing the payment service) of the service recipient used for executing the payment transaction, whether for transferring money or for receiving money.
3. To record if the payment services are granted for business goals or for nonbusiness goals.
4. To act according to <u>one</u> of the following alternatives:

(a) Recording the identification particulars of the service recipient noted in Section 1 will be carried out by copying from the identification document as noted in Section 3 of the Order, or according to an identification document issued by the State of Israel, bearing a name, ID number, date of birth, and picture, which will be kept at the banking corporation. In addition, the banking corporation shall authenticate the service recipient's identification particulars detailed in Sections 2(a)(1) through (3) of the Order with the Population Registry, and is to keep documentation of such examination; the registration of the identification detail required in Section 2(a)(4) of the Order could be done via contacting the Population Registry, provided that the customer's consent is received for that.

(b) Verification vis-à-vis the other banking corporation in which the payment account is managed, and vis-à-vis the banking corporation that issued the means of payment or vis-à-vis a financial institution, that the service recipient is the owner of the payment account and means of payment. The banking corporation is also to verify the

above when there is a change in the payment account details or a change in the means of payment details (to the extent that such changes are known to the banking corporation).

If, when contracting with the service recipient, the banking corporation was unable to authenticate the service recipient's identification details vis-à-vis the Population Registry as required in Section 4(a) or to authenticate that the service recipient is the owner of the payment account or of the means of payment as required in Section 4(b), it may complete the authentication or verification process as soon as possible after setting up the contract, provided that it esablishes a limitation on the activity framework until the requirement is fulfilled.

5. Notwithstanding the provisions of Section 4, to the extent that the payment service allows the accumulation of a balance, and the average balance calculated for a period of 3 months is NIS 5,000 or more, the banking corporation is required to act in accordance with Section 4(a).

6. The provisions of Sections 1-5 shall apply subject to the following conditions:

6.1 The payment account noted in Section 2 is managed by a banking corporation in Israel, and the means of payment noted in Section 2 is issued by a banking corporation in Israel or by a financial institution;

6.2 The total funds transfers caried out in accordance with instructions by the service recipient during a 1-year period does not exceed NIS 100,000;

6.3 The total funds credited to the service recipient during a 1-year period does not exceed NIS 100,000;

6.4 The credit facility extended to the service recipient in a payment card within the framework of the providing of payment services, shall not exceed NIS 20,000 at any given moment;

6.5 The banking corporation shall monitor the activity of the service recipient in regard to the provisions of all laws;

6.6 The manner in which the banking corporation shall implement the provisions of this arrangement, including with regard to the process of verifying the ownership

detailed in Section 4(b), shall be established in accordance with the AML/CFT policy that shall be determined, and that will be anchored in its procedures.

7. The banking corporation shall maintain a computerized database of details of payment and acquiring activities within the framework of providing the payment services. These details shall include the beneficiary name and the payers name (to the extent that such details are known), the amount of the payment or acquiring activity, the goal of the payment activity as provided by the service recipient and the date the payment or acquiring activity is carried out.

8. (a) When the payment service is provided to the service recipient in a banking corporation in which he manages a payment account, the payment service shall be seen as part of the account management and the provisions of this Appendix shall not apply to it, provided that the banking corporation has verified that the reference is to a service recipient who was managing a payment account with it before the beginning of the providing of the service and that all the requirements detailed in Chapter B of the Order were fulfilled regarding it.

(b) If the banking corporation carried out all the requirements detailed in Chapter B of the Order regarding the payment service, the quantitative limitations in Section 6 shall not apply to it.

(c) To eliminate any doubt, it is clarified that when the payment service is provided to a service recipient at a banking corporation on which the identification obligations listed in Section 6a of the Order were carried out, all the requirements of this Appendix shall apply.

9. The provisions of Section 8 shall also apply in a case in which the payment serivce is provided to a service recipient by an auxiliary corporation controlled by a banking corporation that manages the payment account, provided that all the information regarding the customer, including know your customer information, were transferred to it from the banking corporation in accordance with law.

10. To eliminate any doubt, when issuing a payment card, a banking corporation or acquirer may act in accordance with the provisions of Section 6a of the Order.

In this arrangement:

"**Payment Services Law**" – the Payment Services Law, 5779-2019 (hereinafter, the "Payment Services Law");

"**Means of payment**" and "**Payment account**" – as defined in the Payment Services Law;

"**Service recipient**" – an individual who is a resident of Israel;

"**Payment services**" – as defined in the Payment Services Law, except for managing a payment account for a payer or beneficiary whose accumulated balance exceeds NIS 20,000 and except for a current account at a banking corporation;

"**Auxiliary corporation**" – as defined in Section 1 of the Banking (Licensing) Law, 5741-1981.

Financial institution - An entity that holds a license to provide financial services, according to the Control of Financial Services (Regulated Financial Services) Law, 5776-2016, and that as a license holder, its activity is subject to a valid Order, under the Prohibition on Money Laundering Law, 5760-2000, and in accordance with the Combatting Terror Law, 5776-2016.

Appendix B.3

The arrangement established by the Supervisor of Banks in accordance with Sections 6(a)(5) and 7a of the Order:

Notwithstanding the provisions of Sections 2(b), 2(e), and 4(a) of the Order with regard to a banking corporation's obligation to require, from an applicant to open an account, a declaration on benficiaries with an original signature, and despite the provisions of Section 6(a) of the Order regarding a requirement for face to face identification when opening an account managed for a customer, the banking corporation shall act as follows:

(a) It shall authenticate the identification of the customer in the existing account using at least 2 authentication factors, as defined in Section 8 of Proper Conduct of Banking Business Directive no. 367 – "E-banking";

(b) It shall receive from the customer a declaration regarding beneficiaries without an original signature in the managed account;

And provided that the following conditions are met:

(a) The beneficiaries in the managed account and the beneficiaries in the existing account are completely identical;

(b) The customer or the activity in the existing account or in the managed account were not identified as being high AML/CFT risk;

(c) The funds in the managed account will be received from the customer's existing account, in the same banking corporation;

(d) The funds in the managed account will be transferred back to the account owned by the customer in the banking corporation or in another banking corporation.

In this arrangement:

"Customer"—an individual requesting to open a managed account, provided that he holds an account in the same banking corporation that is not an account of types of account noted in Section 7b of the Order ("existing account")

"Managed account"—An account intended for managing investment portfolios, in this regard "managing investment portfolios" – as it is defined in Proper Conduct of Banking Business Directive no. 462—"Customers' Investments in Financial Assets via Portfolio Managers".

Appendix B.4
Arrangement Established by the Supervisor of Banks under Section 7a of the Order:

By force of my authority in accordance with Section 7a of the Order, I hereby determine that with regard to Section 3(a)(1) of the Order, a banking corporation may consider an ID card that includes biometric means of identification that has expired as an ID card, until September 30, 2024.

Appendix B.5
(Temporary provision—Arrangement Established by the Supervisor of Banks under Section 7a of the Order):

By power of my authority according to Section 7a of the Order, I establish that regarding Section 3(a)(1) of the Order, an Immigrant Certificate up to 90 days from its issuance shall be considered as an ID card. This is until June 30, 2024.

Appendix C

Jerusalem, 25 Adar 5775
March 16, 2015
15LM2017

To:
The Banking Corporations
Attn: Chief Executive Officer

Re: Managing risks deriving from customers' cross-border activity

Introduction

1. In recent years we have seen more determined and intensive activity by various countries to locate their residents' funds that are held outside the country of residence. The US has taken steps against banks that managed accounts for US customers and that were suspected of collaborating with those customers to conceal the funds from US tax authorities, and in addition adopted the FATCA legislation in order to receive reports on bank accounts and other financial accounts of Americans outside the US. Said legislation came into effect on July 1, 2014. Other countries such as the UK, Germany, and France also act to receive data on their residents' bank accounts held outside the countries of residence.
2. In July 2014, the OECD published a standard for exchanging data between countries for tax purposes. The goal of the publication was to create a uniform language to the extent possible that will enable countries to exchange information between them for tax purposes, with an emphasis on information on nonresidents' cross activity (that is, information on accounts at financial institutions of a resident of Country A that are managed in Country B, and vice-versa), similar to the arrangement set up by FATCA, which is inherently limited to bilateral relations with the US.
3. The standard may be viewed as an additional pillar in the OECD's Model Tax Convention to avoid double taxation, as it is intended to serve countries interested in regulating bilaterally the priorities in taxation and create a uniform language. The OECD's Model Tax Convention already includes a section on exchange of data, but the innovation is in the level of detail, the due diligence checks, and automation of the reporting, similar to the FATCA regime.
4. On October 27, 2014, the Ministry of Finance notified the OECD that Israel will adopt the said standard by the end of 2018. The announcement also noted that the adoption will be via signing agreements with relevant authorities in various countries. In order to carry out the obligations that Israel will take upon itself, changes in legislation are required.

5. The trend of international collaboration in the battle against tax evasion is liable to increase the exposure of Israeli banking corporations to the compliance risks deriving from cross border activity as well as reputation risk, and obligates them to prepare suitably both in terms of activity vis-à-vis existing customers as well as in accepting new customers, in particular until the international reports are arranged.
6. Proper Conduct of Banking Business Directive 411—"Prevention of Money Laundering and Financing of Terrorism, and Customer Identification" ("**Directive 411**") and the Prohibition on Money Laundering (the Banking Corporations' Requirements regarding Identification, Reporting, and Record-keeping for the Prevention of Money Laundering and the Financing of Terrorism) Order, 5761-2001, establish guidelines and relevant tools related to "Know Your Customer", which enable Israeli banking corporations to reduce the risks involved in activity as detailed in Section 5 above. This letter is intended for implementing what is mentioned there, related to certain activities, with an emphasis on tax liabilities outside the country in which the account was opened, and in the future the requirements will be integrated as part of Directive 411.
7. After consulting with the Advisory Committee on Banking Business, and with the approval of the Governor of the Bank of Israel, I have decided to establish the following requirements:

Application

8. The provisions of Section 9 below are also effective in relation to the banking corporation's activity outside of Israel, with the necessary changes, in accordance with what is listed in Section 3a(b) of Directive 411.

Establishing policy and procedures

9. In light of the increased risks detailed above, and in accordance with the provisions of Section 4–6 of Directive 411, the board of directors of a banking corporation is to examine and update its policy, as well as to verify that management is suitably updating its procedures and controls with regard to the risks inherent in cross-border activity of the banking corporation's customers, with an emphasis on tax liabilities outside the country in which the account was opened, whether the customer is a resident of said country or not, in a risk-based approach, while referring to the following points:

<u>Customer classification</u>

9.1 Classification of a customer as high risk due to cross border activity shall be based on, among other things, the following parameters: the source of the customer's wealth and income and the source of funds that are to be deposited in the account, including receiving appropriate documentation; the extent and type of activity in the account; the customer's manner of organization; private banking; the customer's link to the country in which the banking services are provided; the customer's country of residence;

9.2 Countries in which customer activity therein or fund transfers from them are considered as countries at risk for this matter, such as countries known as off-shore tax shelters;

9.3 A change in identification particulars that may effect the customer's tax obligation.

Required steps

9.4 Receive a declaration from the customer regarding the country or countries in which the customer is a resident for tax purposes, and a declaration that the customer reported income in accordance with the law applicable to said customer, and his or her obligation to notify of any change in tax liability. If necessary, certification should also be requested that that the customer has acted as declared, or alternatively certification that the customer has begun a voluntary disclosure process in the country in which the customer is a resident for tax purposes;

9.5 Receive a waiver on customer confidentiality vis-à-vis authorities abroad;

9.6 Set procedures as well as a scale of authorities for approval of an account's opening, management, and execution of transactions defined as potentially bearing cross-border risk.

In providing banking services to customers subject to FATCA directives, banking corporations are to act to implement them pursuant to the provisions of my letter dated April 6, 2014.

Reasonable refusal

10. Refusal to provide banking services, as detailed below, shall be considered reasonable refusal with regard to the Banking (Service to Customer) Law, 5741-1981:

10.1 Opening an account for a customer who does not cooperate with the banking corporation in a manner necessary to implement the banking corporation's policy and its procedures regarding cross border risk.

10.2 Continued provision of banking services in an existing account, including withdrawal of funds and changing account owner or beneficiaries, in a manner that exposes the banking corporation to the risk of being viewed as collaborating with the customer in order to bypass foreign legislation that applies to the customer.

Start

11. The provisions of this letter begin on the date of its publication.

Provisional directives

12. A banking corporation shall complete the activities noted in Section 9 above, regarding funds of customers in existing accounts, as detailed below:

12.1 Accounts of customers classified by it as high risk customers by December 31, 2015.

12.2 Other accounts by December 31, 2016.

13. The provisions of this circular shall not apply to an account whose owners cannot be contacted due to the relations between the country they are in and the State of Israel.

Sincerely,

David Zaken
Supervisor of Banks

Appendix D

Wage Payments to Palestinian Workers via Bank Transfers

Banking Supervision Department
Office of the Supervisor

Jerusalem, June 30, 2022
Circular No. C-06-2712

Attn: Banking Corporation CEOs

Re: Wage payments to Palestinian workers via bank transfers

1. The scope of bank transfers for wage payments to Palestinian workers is expected to increase relative to the current situation, in view of various processes being advanced by the State of Israel. These include increasing limitations on the use of cash; expiration of the temporary provision regarding the use of cash in transactions with residents of the area or residents of the Palestinian Authority; and the imposing of a requirement on employers to pay wages to Palestinian workers via a non-cash payment. As such, the Bank of Israel is working to promote a process that will enable the banking system to access information in the Population and Immigration Authority regarding Palestinian workers holding a license to work in Israel.
2. After consulting with the Advisory Committee on Banking Business Affairs, and with the approval of the Governor, I have decided to establish the following requirements:
   2.1 According to the Banking Supervision Department's approach, the authentication of information about employees vis-à-vis an official database of the State of Israel, can markedly reduce AML/CFT risk inherent in activity, as it testifies to the absence of information held by security forces in Israel on involvement in terror, and the legality of the employment. Therefore, you are required when conducting a bank transfer for paying Palestinian workers, to authenticate the information about the worker, vis-à-vis the information that

will be made accessible from the Population and Immigration Authority's database.

2.2 This examination vis-à-vis an official database of the State of Israel can replace the examination required by Section 13a(3)(b) of the Prohibition on Money Laundering (The Banking Corporations' Requirements regarding Identification, Reporting, and Record-Keeping for the Prevention of Money Laundering and the Financing of Terrorism) Order, 5761–2001.

2.3 In view of the above, the banking system is required to complete the preparation for using information that will be made accessible from the database of the Population and Immigration Authority and to provide wage payment services via bank transfers at notable scopes of activity, by October 31, 2022 at the latest.

2.4 To the extent that an obligation will be imposed on employers to pay wages via bank transfer, the Banking Supervision Department will view the money transfer service as part of managing the account, and therefore in terms of the banks' refusal to provide the service shall be done with attention paid to the provisions of Section 2 of the Banking (Service to Customer) Law, 5741-1981, meaning a refusal to provide the service can only be if it is reasonable.

3. Application—Section 2.4 of my letter shall not apply to a foreign bank.
4. The Banking Supervision Department shall examine later on the integration noted in this letter in the framework of Proper Conduct of Banking Business Directive no. 411 (Management of Anti-Money Laundering and Countering Financing of Terrorism Risks).

Respectfully,

Yair Avidan
Supervisor of Banks

Updates

Circular 06 no.	Version	Details	Date
1104		Original circular	December 8, 1983
-----	1	Integration into Proper Conduct of Banking Business Directives	August 1991
1731	2	Update	Octoner 11, 1994
1745	3	Update	January 25, 1995
1794	4	Update	December 26, 1995
-----	5	New version of Proper Conduct of Banking Business file	December 1995
1924	6	Update	May 25, 1998
2076	7	Update	May 2, 2002
2157	8	Update	February 1, 2005
2217	9	Update	December 2007
2257	10	Update	January 24, 2010
2288	11	Update	January 12, 2011
2321	12	Update	December 26, 2011
2467	13	Update	June 9, 2015
2505	14	Update	October 30, 2016
2519	15	Update	November 23, 2016
2531	16	Update	March 6, 2017
2610	17	Update	March 12, 2020
2629	18	Update	October 4, 2020
2669	19	Update	September 30, 2021
2677	20	Update	October 24, 2021
2706	21	Update	May 9, 2022
2723	22	Update	September 19, 2022
2729	23	Update	December 5, 2022
2748	24	Update	June 11, 2023
2770	25	Update	December 31, 2023