E-Banking

Table of Contents

Chapter		Page
Chapter A	**General**	
	Introduction	3
	Applicability	5
	Definitions	5
Chapter B	**Corporate Governance**	
	Board of directors	8
	Senior management	9
Chapter C	**Opening an Online Account and Signing up for E-Banking Services**	
	Opening and managing an Online Account	10
	Opening and Managing a Long-Term Savings Account for a Child	16
	Agreement to provide E-Banking services	17
	Signing up for E-Banking services remotely	19
	Establishing an agreement remotely	19
Chapter C1	Adding and removing an account holder and authorized signatory remotely	
Chapter D	**Identification and Authentication**	21
Chapter E	**Protection of Customers**	
	Monitoring exceptions and high-risk transactions	22
	Alerts to customers	22
	Customer guidance	24
	Customer support center	24
Chapter F	**E-Banking Controls**	
	Updating of account information	25
	Transfers, payments and other transactions	25
	Securing communication channels	26
Chapter G	**Controls for Specific Channels and Devices**	
	Email activity	26
	Short Message Service (SMS)	27
	Use of mobile devices	28
	Automated Teller Machines (ATM)	28
	Instructions for conducting phone transactions by human response	28
Chapter H	**Account Aggregation**	28
Chapter H1	**Transferring Information regarding the Balance in a Current Account**	29
Chapter I	**Reports and Approvals**	
	Issues requiring reporting	31
	Issues requiring approval	31
Chapter J	**Transitional Provisions**	32

Appendix A	**Signing up Remotely for E-Banking Services: Extensions to Additional Cases**	Cancelled
Appendix B	**Opening and Managing a Long-Term Savings Account for a Child**	Cancelled
Appendix C	**File Format for Transferring Information on Customer's Balance in a Current Account**	35

Chapter A: General

Introduction

1. In recent years, customers of banking corporations increasingly use technology and direct channels to consume banking services. This phenomenon is also evident worldwide. Expanding E-Banking services and the types of services including banking via the Internet, telephone and using Automated Teller Machines (ATMs), makes it possible to reduce the prices of services to customers, and makes it easier for them to manage their activity independently and conveniently anywhere, at any time, through various channels, and regardless of the working hours of the branches of their banking corporation. Furthermore, the development and expansion of E-Banking services are expected to enable banking corporations to become more efficient over time.
2. In addition to the abovementioned benefits of E-Banking, increasing the scope of banking services through technology and allowing customers to conduct banking activity remotely potentially increase the unique risks inherent in such activity, including information security risks and cybersecurity risks, invasion of privacy risks, fraud and embezzlement risks, compliance risks, money laundering risks, legal risks and reputation risks.
3. To deal with these risks, banking corporations need to reinforce and adapt their risk management framework to the advanced technological operating environment and update it regularly and dynamically, due to the speed at which technology is evolving, while adhering, at all times, to information security principles, including, *inter alia*, maintaining confidentiality of customer information and privacy protection, data integrity and the availability of E-Banking services. It should be clarified that a banking corporation that is subject to the provisions of the Proper Conduct of Banking Business Directives: Directive no. 310 on Risk Management, Directive no. 350 on Operational Risk Management, Directive no. 357 on Information Technology Management, and Directive no. 361 on Cyber Defense Management, is required to do so in accordance with these directives.
4. In addition, banking corporations are required to develop and improve methods for detecting fraud and embezzlement, for prevention of money laundering, and

for handling failures in a swift and adequate manner, so as to minimize harm to the customer, legal risks and reputational risks associated with E-Banking activities and arising from the increase in the quantity and scope of the databases.

5. This directive regulates the activity of the banking corporations in providing E-Banking services to customers. The directive enables banking corporations to offer their customers banking services, from opening an account remotely without having to reach the banking corporation's branch, issuing a payment card subject to the provisions of any law, signing up for E-Banking services online even for an existing account, through to conducting ongoing activity, without having to arrive at the branch. This directive thus enables customers and the banking corporations to expand their digital activities and enjoy its advantages as aforementioned, and makes it easier for new players, that do not have a network of branches, to engage in financial activity, thereby increasing competition. However, expanding the possibilities for remote banking activity is contingent on enhancing and improving risk management and the controls exercised by the banking corporations, such as controls for customer identification and authentication, initiating and sending alerts to customers and monitoring anomalies in this type of activity at the customer level and at the bank level.
6. To provide an end-to-end solution for full banking activity and reduce the customers' need to arrive at the branch, banking corporations are required to examine options to offer their customers complementary services, all within the limits prescribed by law and regulation.

Application

7. (a) This directive shall apply to the following corporations as defined in the Banking (Licensing) Law, 5741-1981 (hereinafter, "Banking Corporation");
   (1) banking corporation;
   (2) a corporation as provided in Sections 11 (a), (3a), and (3b);
   (3) a corporation as provided in Section 11 (b);
   (4) a merchant acquirer as defined in Section 36i.

   (b) Cancelled.

Definitions

8.

"Account Holder"	As the term is defined in Section 1 of the Order.
"Portfolio Management License Holder"	One who holds a portfolio manager's license in accordance with the Regulation of Investment Consulting, Investment Marketing, and Investment Portfolio Management Occupation Law, 5755-1995.
"Authentication Factor"	One of the following: (a) An item in the user's possession (e.g., a **one-time password (OTP)** generated by a hardware component in the user's possession that is linked to his or her account, a temporary one-time password generated by the banking corporation and delivered to the customer by Short Message Service (SMS)—including a voice message—or a digital certificate stored on a smart card or another component in the user's possession); (b) An item known only to the user (e.g., a fixed password); (c) An item that is the user (including a biometric characteristic, such as voice print, fingerprint or facial recognition).

The "Order"	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.
"Credit Card Company"	An auxiliary corporation referred to in Section 11(b) of the Banking (Licensing) Law, 5741-1981.
"Online Account"	An account as defined in the Order, opened in accordance with this directive.
"Discounting Account"	A concentration of debits and credits under the authority of the contractual agreement to provide discounting services on transactions carried out via payment card; in this regard, "payment card"—as defined in the Order.
"Acquiring Account"	A concentration of debits and credits under the authority of the contractual agreement to acquire transactions executed with a payment card; in this regard, "payment card"—as defined in the Order.
"Electronic signature"	As defined in the Electronic Signature Law, 5761-2001.
"Beneficiary"	Except a beneficiary created in accordance with Proper Conduct of Banking Business Directive no. 439.
"Authorized Signatory"	As the term is defined in Section 1 of the Order.
"Mobile Device"	Including a laptop computer, a tablet computer, a mobile phone.
"Voice Message"	A Short Message Service notice received on the customer's mobile telephone as a voice message.
"E-Banking"	Banking services provided by one or more of the following channels: (a) Internet channels, including: (1) A website; (2) An application;

(3) Email;

(4) Instant Messaging services (IM);

(b) Landline and mobile telephony channels, including:

(1) Human response;

(2) Interactive Voice Response (IVR);

(3) Short Message Service (SMS) /

(4) Fax

(c) Automated Teller Machines (ATM)

"Banking Services"	As defined under "Service" in the Banking (Service to Customer) Law, 5741-1981, (hereinafter, the "Banking (Service to Customer) Law"), including the receipt of information, account aggregation, execution of transactions and providing instructions to execute transactions.
"Discounting Services"	As defined in Section 7a.(a) of the Banking (Service to the Customer) Law, 5741-1981.
"Corporation"	As defined in Subsection (1) in the definition of corporation in Section 1 of the Order.

Chapter B: Corporate Governance

Board of directors

The Board of Directors is responsible for:

9. Ensuring that all risks inherent in E-Banking, including information security risks and cybersecurity risks, invasion of privacy risks, fraud and embezzlement risks, legal risks, compliance risks, money laundering risks, reputational risks and strategic risks are managed according to the principles set forth in Proper Conduct of Banking Business Directive no. 310 on "Risk Management" and Proper Conduct of Banking Business Directive no. 350 on "Operational Risk Management" and in accordance with the various specific directives, including Proper Conduct of Banking Business Directive no. 357 on "Information Technology Management" and Proper Conduct of Banking Business Directive no. 361 on "Cyber Defense Management".
10. Reviewing and approving a risk management framework for E-Banking to be anchored in a policy document.

    The policy shall address, *inter alia*, the following issues:

    (a) Communication channels as well as products and types of services permitted in each of the communication channels;

    (b) Principles and parameters for classifying E-Banking transactions by risk level, both at the individual transaction level and laterally, on the basis of which the mandatory means of identification and authentication shall be determined, *inter alia*, subject to the law or regulation;

    (c) Opening and managing an Online Account, taking into account, *inter alia*, the controls, restrictions and additional documents in addition to those prescribed in this directive, in accordance with the risk-based approach, in order to mitigate the risks involved in this activity, both at the individual account level and at the banking corporation level.

    (d) E-Banking controls, including:

        (1) Identification and authentication of customers, *inter alia*, by type of customer, type of transaction and level of inherent risk;

(2) Monitoring of exceptional activity (anomalies), at the customer level and at the bank level, high-risk transactions and sending alerts to customers;

(3) Increasing customer awareness and providing them with guidance;

(4) Controls over specific channels;

(5) Principles of E-Banking information security between the customer and banking corporation.

11. Ensuring that risk management of first and second lines of defense for E-Banking are reviewed periodically by the internal audit function, based on the guidelines outlined in Directive 307, Internal Audit Function, provided it applies to the corporation.
12. To prescribe the reporting required for E-Banking, including significant failures in providing services and handling them.

Senior management

Senior management is responsible for:

13. Developing and integrating a policy to anchor the risk management framework for E-Banking.
14. Ensuring that clear areas of responsibility have been defined and adequate resources have been allocated for risk management in E-Banking, including managers and employees with appropriate skills and experience.
15. Implementing processes for supervision of integrating the E-Banking risk management framework, including: reports on risk assessment results and assimilation of appropriate controls, results of the monitoring processes in key systems and significant failures in the availability of E-Banking systems.
16. Developing a plan for taking ongoing actions to increase customers' awareness of the risks inherent in E-Banking activity.
17. Following the technological developments in the E-Banking field and the risks involved in them.

Chapter C: Opening an Online Account and Signing up for E-Banking Services

Opening and Managing an Online Account

Principles of opening an online account

18. A banking corporation may allow the opening of an online account in accordance with the following rules:
    (a) The online-account applicant shall be an individual resident of Israel who is at least 16 years of age or is a corporation.
    (b) The applicant or applicants wishing to open an account shall be its account holders, and there shall be no beneficiaries in the account other than the account holders.
    (c) A banking corporation that is not a credit card company, shall assign the account that was opened to a branch and send a notice to the customer with the details of the branch to which the account was assigned.
    (d) In addition to the provisions of Subsections (a)–(c), opening an account for an individual resident of Israel who is less than 18 years of age (hereinafter, a "minor") shall be subject to the following stipulations:
        (1) In the process of opening an account for a minor, the banking corporation is to verify that before the account is opened, the minor shall have the opportunity to receive explanations and responses to questions he or she may have with regard to this process from a representative of the banking corporation, through a remote face to face or telephone interaction in real time. During the course of the process of opening an account for a minor, the banking corporation shall provide a face to face explanation to the minor on the manner of managing the account, with an emphasis on the unique characteristics of a minor's account.
        (2) All the relevant guidelines in Proper Conduct of Banking Business Directive no. 416 on "Minors' Accounts"

(hereinafter, "Directive 416") shall be followed, with the following adjustments:

The prior written consent of the minor's representative as required in Section 6(a) of Directive 416 with regard to overdrawing the minor's account, and as required in Section 11 of Directive 416 with regard to issuing a credit card to a minor, can be given after the following checks:

a) Identification and authentication of the minor's representative, which will be carried out in one of the ways detailed in Section 19 of this Directive.

b) Authentication that the person identified and authenticated as aforementioned is authorized to serve as the minor's representative.

(e) The banking corporation shall digitally document all the face to face identification and authentication processes regarding an online-account applicant who is an individual, and of the authorized signatory acting on behalf of a corporation requesting to open an account, and of the minor's representative in case his or her consent is required in accordance with Subsection (d)(2) above, the "Know Your Customer" process that it carried out, the declaration of beneficiaries in the account, the declaration of the holder of control in the corporation, and all the documents presented within this framework. Such documentation shall be considered "identification documents" with regard to Section 7 of the Order, entitled "Keeping the Identification Documents".

(f) In addition to the provisions of Section 50 of Proper Conduct of Banking Business Directive no. 411 on "Management of Anti-Money Laundering and Countering Financing of Terrorism Risks", a banking corporation that identifies, while opening or managing an online account, that it is of a high risk customer, is permitted to not open an online account or to block the activity in an existing account, as relevant.

(g) The banking corporation is to outline the unique risks inherent in the process of opening an account online, for both the banking corporation and its customers, individual or corporation, including remotely adding or removing an account holder or authorized signatory, and it shall establish ways to reduce the exposure to the banking corporation and to the customer, including stopping the online process and referring the customer to the branch if necessary.

Identification and authentication of the online account applicant

19. Identification of the online account applicant, and in the case of a corporation the authorized signatory in the account as well, and the authentication of the identity details may be carried out through one of the following methods:

(a) Based on the applicant's ID card that is presented to the bank when opening the account, while using technology for remote face-to-face identification and authentication, as detailed in Section 27a below.

(b) Based on the applicant's ID card and an additional identifying document issued by the State of Israel, that bears the customer's name, ID number and date of birth, that were presented when opening the account, together with:

(1) Use of video conferencing technology

(2) Execution of a bank transfer through an account under the name of the online-account applicant, at a banking corporation in Israel, except for the following cases:

a) Opening an account via the banking corporation's website, through an existing account, and after authenticating the customer via at least 2 authentication factors.

b) Opening an online account that is a loan account, at an amount of up to NIS 50,000, provided that the amount of the loan shall be transferred to an account under the name of the loan account applicant, at a banking corporation in Israel.

(c) Without derogating from the generality of the provisions of Subsection (a) of this Section, when opening an online account per Subsection (b), which is an acquiring account in which the annual acquiring turnover does not exceed NIS 50,000 or which is a discounting account in which the annual turnover of transactions for which discounting services are provided through it does not exceed NIS 50,000, the banking corporation is permitted to not make use of video conferencing technologies, notwithstanding the provisions of Subsection (b)(1) of this Section, provided the amount of the acquiring funds or discounting funds, as relevant, is transferred to an account under the name of the acquiring account applicant or the discounting account applicant, as relevant, at a banking corporation in Israel.

If the annual acquiring turnover increases to over NIS 50,000, or if the annual turnover of transactions for which discounting services are provided through it increases to over NIS 50,000, the banking corporation shall establish a threshold up to which it will continue to provide acquiring services or discounting services, as relevant, to the customer, and will act to complete the customer identification and authentication process so long as it has not already done so previously, within a reasonable amount of time given the specific conditions, through the following means:

(1) Use of video conferencing technology.

(2) The transfer of a random amount to an account at a banking corporation in Israel under the name of the acquiring account applicant or the discounting account applicant, out of the amount of funds that the banking corporation is required to credit the customer the first time that acquiring funds or discounting funds are to be credited.

If necessary, the banking corporation will carry out a "Know Your Customer" process as detailed in Sections 20–21 below, updated in accordance with the expected activity in the account.

(d) With regard to a corporation, based on the corporation's registration certificate that was signed electronically by the Israeli Corporations

Authority or a certified copy thereof as defined in Section 3(b)(2) of the Order signed with an electronic signature that complies with the purposes of the provisions of the Order in this matter, and that was presented when opening the account.

The provisions of Subsections (a)–(c) above do not derogate from the other obligations detailed in Section 3(a)(1) of the Order.

Corporate documents requirements

19a. When opening the account, the banking corporation shall receive the documents required in Section 3(a)(3) of the Order and shall document them; a certified copy as defined in Section 3(b)(2) of the Order and a lawyer's certification as noted in Sections 3(a)(3)(d) and 3(a)(3)(e) of the Order may be accepted in online form as well when they are signed with an electronic signature that complies with the purposes of the provisions of the Order in this regard.

Know Your Customer

20. Cancelled.

21. The banking corporation may carry out the "Know Your Customer" procedure via technological means other than those it uses for identification and authentication, provided it adopted means to verify that the respondent to the "Know Your Customer" questionnaire is the same as the customer identified and authenticated in accordance with Section 19 of this Directive, and in a corporate account that the respondent to the questionnaire is the authorized signatory to it.

Declaration of beneficiary and holder of control in an online account

22. The banking corporation shall require that the customer or the corporation's authorized signatory requesting to open an online account sign a declaration of beneficiaries online, and in addition shall document the customer or the corporation's authorized signatory declaring, in his or her voice, that there are no beneficiaries in the account other than the account holder.

In the case of opening an account for a corporation, the banking corporation shall require, in addition, that the authorized signatory sign an online form

declaring a holder of control, and will document the authorized signatory declaring in his or her voice regarding the veracity of the form.

Restrictions on an online account

23. An online account, including an account in which an account holder was added remotely, shall be marked and identified as an online account in the banking corporation's computer systems, to monitor risks and enhance monitoring for a period to be determined by the banking corporation in accordance with a risk assessment.
24. Cancelled.
25. Cancelled.
26. Cancelled.
27. A banking corporation may remove the restrictions on an account that was opened online, including those that were imposed on an account in which an account holder was added remotely, as described in this part, after completing the full identification of the customer or of the authorized signatory in the case of a corporate account, in accordance with the provisions of the Order.

Technology for remote face-to-face identification and authentication

27a. A banking corporation that carries out identification and authentication of an applicant to open an account pursuant to Section 19(a) of this Directive, shall act in accordance with the following sections:

(a) The banking corporation shall use technology for remote face to face identification and authentication via face to face interaction in real time or via video recording that is not in real time, and which is integrated at least with the following types of controls:

(1) Checking the originality of the certificate presented, for authentication, based on the permanent characteristics of that certificate.

(2) Authenticating that the certificate presented is in fact the certificate of the persons identifying themselves through the technology, including authentication through comparing the picture on the certificate with the picture of the persons identifying themselves via the technology.

(3) Authenticating the details of the persons identifying themselves through the technology, as they are read from the certificate presented, against the relevant databases, including the authentications required in Section 3(a) of the Order.

(4) In a case in which the use of said technology, which does not require face to face interaction in real time, the following should be integrated, in addition to the controls noted above:

a) Liveness detection.

b) Carrying out an ongoing control process on a sample of accounts that have been opened, as soon as possible after the account is opened. In a case of an account that is classified as an account at high AML/CFT risk, the control process shall be carried out before allowing the customer to act in the account.

In this regard:

"Control process"—an examination by a banking corporation representative regarding to the adequacy of the process implemented, including the comprehensiveness of the data submitted by the customer during the account opening process;

"Sample"—a sample that shall include all the accounts classified as accounts at high AML/CFT risk as well as additional accounts out of all the accounts opened that will be chosen via a risk-based approach; the share of the sample shall not be less than 20 percent of all the accounts opened.

(a1) The types of controls detailed in Subsection (a)(2) and in Subsection (a)(4)a. above, shall be carried out together, without a break in between them.

(b) The banking corporation is to establish minimum technological thresholds that said technology will have to comply with, so that it will be able to be relied upon for the purpose of opening an online account.

(c) Said technology will make it possible to save the digital documentation as detailed in Section 18(e) above, for the period set in Section 7 of the Order, at least.

Opening and Managing a Long-Term Savings Account for a Child

27b. The following provisions of this Directive—Sections 18–27a, Sections 29(b)–39, Section 42(d) regarding a change in contract details, and Section 57—shall not apply to a long-term savings account for a child (hereinafter, the "Savings Account"), which is opened under Article E to Chapter D of the National Insurance Law [Consolidated Version], 5755-1995, and the National Insurance (Long Term Savings for a Child) Regulations, 5776-2016, enacted thereunder (hereinafter: the "Regulations").

(a) A banking corporation may open a savings account and sign up the account to E-Banking services based on the identification details transferred to it through a computerized record by the National Insurance Institute, without requiring additional identification details.

(b) (1) On opening a savings account, the banking corporation may sign up the customer to E-Banking services, to a channel or a bundle of channels chosen by the banking corporation from time to time, without the customer's having chosen them. The customer may terminate the agreement to obtain a service, channel or a bundle of channels at any time.

(2) The banking corporation shall present in the E-Banking services agreement the services permitted in each channel, the risks associated with using these services, and shall bring to the attention of the customer the principles of information security and privacy protection recommended for implementation by the customer, in order to minimize these risks.

(3) Signing up for online message services in accordance with Proper Conduct of Banking Business Directive no. 420 on "Sending Notices via Means of Communication" (hereinafter, "Directive 420") requires an explicit request by the customer.

(c) When establishing a savings account agreement, including an E-Banking agreement, the banking corporation may regard the National Insurance Institute notice regarding the opening of an account as the customer's approval that he

has been given the opportunity to read the agreement and has agreed to its terms and conditions. The version of the agreement established with the customer shall be available for him to review at any time, in a clear and easily readable form and in printable format.

(d) Changing the contact details shall be made possible by using at least one authentication factor, or the use of identification details and several questions whose answers the banking corporation deems sufficient to allow customer authentication.

(e) "Parent" and "beneficiary child" in this section, as defined by the Law and Regulations.

Agreement to provide E-Banking services

28. A banking corporation shall reach a contractual agreement with a customer to provide E-Banking services (hereinafter: "E-Banking Agreement").

29. Notwithstanding the provisions of Section 28 above:

(a) A banking corporation may provide information to the customer on his accounts via human response, even if the customer is not a party to an E-Banking Agreement.

(b) A banking corporation may send notices as detailed below even if the customer is not a party to an E-Banking Agreement for that channel:

1. Notices via Short Message Service (SMS), including a voice message, in order to send a temporary One Time Password;
2. Alerts and requests for approvals as noted in Sections 48–51 below;
3. Notices regarding transferring information regarding the balance in a current account, per the provisions of Section 73a(4) below.

(c) A banking corporation shall not be required to establish an E-Banking Agreement with a person using the corporation's Automated Teller Machines (ATM) to obtain occasional service, such as payment of vouchers or cash withdrawal.

30. With regard to a customer sending notifications to an issuer, the relevant law is the Payment Services Law, 5779-2019, and the regulations by its authority, even if the customer is not party to an E-Banking Agreement.

31. The banking corporation may offer its customers a channels and services package under the agreement, provided that the customers shall be allowed to select channels they are not interested in. The aforesaid shall not apply in a case where a bundle of channels is necessary for providing a particular service. The customer may terminate the agreement to obtain a service, a channel or a bundle of channels at any time.
32. Prior to the customer's approval of the agreement, the banking corporation shall introduce the E-Banking services permitted in each channel, the risks associated with using these services, and will bring to the attention of the customer the principles of information security and privacy protection the customer is advised to implement, in order to minimize these risks and the customer's right to terminate the contract to receive the services at any time. In a case in which the customer signed an e-banking agreement including future services or channels that the banking corporation will offer, and the service or channel is not offered to the customers at the time of the contract and the risks related to the use of the service or channel were not brought to the customer's attention, the banking corporation shall fulfill the provisions of this section before the customer's initial use of the service or channel.

Signing up for E-Banking services remotely

33. A banking corporation may sign a customer up for e-banking services using means of identification and authentication in accordance with the risk assessment and policy authorized by the board of directors, provided that said use is consistent with the provisions of Chapter D below.
34. Cancelled.
35. Cancelled.
36. Cancelled.
37. Cancelled.
38. Termination of E-Banking service shall be made using the same level of identification and authentication used for receiving the service in accordance with Section 40 below.

Establishing an agreement remotely

39. When establishing an agreement remotely, the banking corporation shall use means to ensure that the customer has been given the opportunity to read the agreement and has agreed to its terms and conditions. The version of the agreement that the customer has approved shall be available for him to review at any time, in a clear and easily readable form and in printable format.

Chapter C1: Adding or removing an account holder or authorized signatory remotely

39a. A banking corporation may enable its customers to remotely add or remove an account holder or authorized signatory in accordance with the following rules:

(a) Identification and authentication of the identification particulars of each of the following, as relevant: one requesting to add an account holder or authorized signatory (hereinafter, "the adder"), one requesting to remove an account holder or authorized signatory (hereinafter, "the remover"), one requesting to join as an account holder or authorized signatory (hereinafter, "the one being added"), or one requesting to be removed from the account in which he is listed as account holder or authorized signatory (hereinafter, "the one being removed"), shall be in accordance with the guidelines in Sections 19(a)–(b) of this Directive, except for Section 19(b)(2) that applies only to the one being added as account holder or authorized signatory.

(b) Notwithstanding the provisions of Subsection (a) above:

(1) When adding or removing an authorized signatory in a corporate account, there will not be an obligation to identify the adder or the remover of the one being removed. Instead, the corporation shall present a certified copy of the decision of the competent function at the corporation as defined in Section 3(b)(2) of the Order or a lawyer's certification of the addition or removal of an authorized signatory in the account, and these can be received online as well

when signed with an electronic signature complying with the purposes of the provisions of the Order in this regard.

(2) The identification and authentication of the identification particulars of the one requesting to add or remove an authorized signatory who has qualifications imposed on him that prevent him from carrying out transfers, payments, or other activities to beneficiaries, as well as someone with power of attorney to manage investment portfolios who holds a portfolio management license, can be carried out through at least two authentication factors as well.

(c) Identification of the adder or remover and the authentication of their identification particulars, as well as the identification of the one being added or the one being removed and the authentication of their identification particulars do not have to be in the same appointment, provided that the banking corporation adopted measures to verify that the one who was identified and authenticated as the one being added or the one being removed as noted is in fact the one being referred to in the request to add or remove.

(d) All the provisions related to an applicant to open an online account in Chapter C above, shall apply, with the necessary changes and in accordance with all laws, on the adder, remover, the one being added and the one being removed.

(e) Adding or removing an account holder remotely shall not be permitted in a corporation's account. In this section, "corporation" is as it is defined in the Order.

(f) Regarding one with a power of attorney to manage investment portfolios—it will not be possible to remotely add someone who does not have a portfolio management license.

Chapter D: Identification and Authentication

40. A banking corporation shall determine the means of personal identification and authentication for its E-Banking activity in accordance with the risk assessment and policy approved by the Board of Directors.

41. A banking corporation shall implement processes on how each means of identification and authentication is created, delivered, operated and replaced, so as to allow it to ensure, *inter alia*, that sensitive information is not revealed in the creation and delivery process. Regarding the use of passwords, rules shall be established on the manner of determining the password's length and composition, restrictions on reuse, frequency of replacement, blocking and releasing passwords.

42. Transactions defined as high risk, in accordance with the principles approved by the Board of Directors, will be allowed following authentication by at least two authentication factors.

    A high-risk transaction shall include, at a minimum:

    (a) Transfers, payments and transactions over the first limit threshold established by the banking corporation in accordance with Section 60 (a) below;

    (b) Cancelled.

    (c) Cash withdrawals from Automated Teller Machines (ATMs).

    (d) Change of the contact details or the name of the account holder in accordance with Sections 57–58 below.

    (e) Adding or removing an authorized signatory upon whom there are qualifications that prevent them from carrying out transfers, payments, or other activities to beneficiaries, in accordance with Section 39a(b) of this Directive.

    (f) Adding or removing one with power of attorney to manage investment portfolios, who has a portfolio management license, in accordance with Section 39a(b) of this Directive.

43. When the consent of all partners to the account is required for carrying out a transaction or to give an order to perform a transaction, such consent will be required for E-Banking as well.
44. Notwithstanding Section 43 above, a banking corporation may reach an agreement with a customer which is a corporation, that those authorized by the customer will act alone where E-Banking services are concerned, even in cases where authorization to operate the account outside the framework of E-Banking services are different, subject to the authenticated approval of a competent officer of the corporation.

    In this Section, "corporation" is as it is defined in the Order.

Chapter E: Protection of Customers

Monitoring exceptions and high-risk transactions

45. A banking corporation shall implement an automatic mechanism to identify and monitor anomalous activity in the accounts of customers, and in particular high-risk transactions for the purpose of detecting suspicious activity in real time.
46. When detecting anomalous activity, use will also be made of segmentation by groups of customers or accounts, such as: Online Accounts and accounts that were signed up for E-Banking services online.
47. A banking corporation shall follow the development of E-Banking fraud methods and threats in Israel and worldwide, and shall update the monitoring mechanism as needed. To this end, the banking corporation shall use the information it receives from internal and external sources (including the police and security services and information security companies).

Alerts to customers

48. A banking corporation shall alert the customer regarding anomalous activity it has detected as stated in Section 45 above, on transactions executed at the banking corporation's discretion, and in any case on adding a channel or service that is not solely for information. It shall also consider taking

immediate measures, such as the immediate suspension of a transaction or obtaining the customer's re-approval for the transaction.

49. The alerts and requests for re-approval shall be delivered on a different channel or a different device than the one used to carry out the transaction, shall contain the minimum transaction details required in order to identify it, but shall not include full identifying details about the account, customer or payment card.
50. The channel shall be selected taking into account the speed at which the alert is required to be delivered to the customer, the level of risk inherent in the transaction, as well as the level of information security required depending on the level of sensitivity of the information transmitted, unless the customer has chosen a specific channel or device to receive alerts and request approvals and provided that Section 49 above is met. However, regarding alerts sent to customers regarding anomalous activity defined as noted in Section 45 above, and subject to the provisions of Section 49 above, the banking corporation will be able to contact the customer through the channel of device it chooses, in addition to the channels or device the customer chooses.
51. If an account has several holders, the banking corporation shall notify all holders of anomalous activity.

Customer guidance

52. A banking corporation shall clarify to its customers the main risks involved in obtaining E-Banking services and its recommendations on taking reasonable security measures when using such services.
53. The clarification shall be delivered through a variety of channels, such as: the bank's website, notices on accessing E-Banking services, email and bulletins.
54. A banking corporation shall manage the risk involved in fraudulent websites or applications, and when there is a suspicion of other scams designed to make customers divulge sensitive information such as their account number, passwords or payment card information, to unauthorized parties.
55. If there is suspicion of an E-Banking fraud which may affect numerous customers in a short time frame, at the same time as removing the threat and reducing the potential damage, the banking corporation shall notify its

customers who are at risk and consider informing the general public, as appropriate.

Customer support center

56. A banking corporation shall have a customer support center, which shall include human response, to support the activities of E-Banking customers.

Chapter F: E-Banking Controls

Updating of account information

57. Changing contact details (such as mobile phone number, email address and postal address), shall be possible following authentication using at least two authentication factors.
58. Updating the name of the account holder shall be allowed after using at least two factors of authentication and presenting a copy of the identification and authentication documents, as appropriate, required under Section 3 of the Order.
59. A banking corporation shall enhance the monitoring of accounts in which anomalous activity has been detected in terms of remote updating of account information for a period to be determined following a risk assessment.

Transfers, payments and other transactions

60. A banking corporation shall set limits on amounts of transfers, payments and other transactions to beneficiaries, as follows:
    (a) A maximum amount, within which personal means of identification and authentication as established by the banking corporation in accordance with the risk assessment and policy approved by its board as noted in Section 40 above, shall be required;
    (b) A maximum amount, which—between the maximum amount in Section (a) above and that amount—shall require the use of two factor authentication;
    (c) Beyond the maximum amount in Section (b) above, the use of technology that combines identification and authentication of the user, secrecy and data integrity and prevention of denial shall be required.
61. Determining these amounts shall be based on a risk assessment that takes into account, among other things, the beneficiary's identity, type of customer and his or her modus operandi.
62. A banking corporation shall establish adequate policies and controls to minimize the risk of unauthorized transfers, including, for business customers,

the option for a control that requires the approval by two persons to carry out any transfer.

Securing communication channels

63. A banking corporation shall use an encryption algorithm to protect the information of its customers being transferred through external networks, including the Internet and excluding telephone networks.

64. Notwithstanding the provisions of Section 63 above:

    (a) A banking corporation may send alerts and requests for approval as stated in Sections 48 and 49 above, without using an encryption algorithm.

    (b) Repealed.

65. A banking corporation shall examine the need to implement measures to ensure the integrity of the message content and prevention of denial of the transfer of information.

Chapter G: Controls for Specific Channels and Devices

Email activity

66. Notwithstanding the provisions of Section 63 above, and subject to carrying out an appropriate risk assessment, a banking corporation is not required to use an encryption algorithm in order to protect its customers' data passing via email, from the banking corporation to the customer and vice versa. Within the framework of this risk assessment, the banking corporation shall determine the level of security required for the various types of information and activities that it predefines as necessary to be transferred and executed via email, and all in accordance with the following principles:

    (a) The risk assessment shall refer to, among other things, the following aspects: customer type, sensitivity and confidentiality of the information, frequency and scope of the transmission of the information, and in addition an assessment of the level of security of the customer's email service as far as possible.

    (b) The level of security required shall also refer to, among other things, the following aspects: the need to encrypt the information and the required

strength of the encryption, the extent of the need to unambiguously identify the customer sending the email, including full identifying details of the customer or the account in the information sent.

(c) Implementing current and periodic appropriate controls related to activities and types of information that the banking corporation approved to send via email, referring to, among other things, various aspects of diagnosing, preventing and handling information leakage should it be discovered.

It is clarified that the provisions of this section do not apply to alerts and authorization requests as noted in Section 64 above.

Short Message Service (SMS)

67. (a) Transmission of information via Short Message Service (SMS) shall not include full identifying details about the customer and the customer's account details (such as the customer's name, customer's account number, payment card number).

(b) A banking corporation that uses a temporary one-time password sent via Short Message Service as an authentication factor shall provide a solution to those customers who are unable to receive such a message, or who are unable to read it, by sending a voice message.

Use of mobile devices

68. A banking corporation shall identify and assess the specific risks embodied in the use of a mobile device, including loss or theft of the device, and shall determine security measures to deal with these risks.

69. A banking corporation shall instruct its customers regarding the use of mobile devices, including the need for their physical and logical security and the need to lock the device. In this respect, customers shall be instructed on how to act in case of a theft, loss or misuse of a mobile device, particularly when the device is used for receiving alerts and requests for approval of transactions. A banking corporation shall provide its customers with a phone number for reporting, if necessary, so the bank can block alerts through that channel.

70. Additional controls will be established to enable customers to obtain or create a temporary one-time password (OTP), since the effectiveness of 2FA decreases when the device is used for both communicating and receiving or creating an OTP.

Automated Teller Machines (ATM)

71. A banking corporation shall implement control measures to help, among other things, prevent and identify fraud at Automated Teller Machines (ATM), including:
    (a) An adequate audit trail, including proper documentation of the system;
    (b) Full functional support for smart card transactions in Automated Teller Machines (ATM) used to withdraw cash.

Instructions for carrying out transactions via telephone by human response

72. Instructions for performing transactions via telephone by human response shall be recorded in records that shall include, *inter alia*, the date on which the order was given, the details of the clerk who received the order and a specific indication that the order was given by telephone.

Chapter H: Account Aggregation

73. A banking corporation may offer its customers a service of "account aggregation" (hereinafter: the "Service") under the following conditions:
    (a) The Service shall be limited to information aggregation only.
    (b) The banking corporation and its employees shall have no access to customer information obtained from other banking corporations (hereinafter: "Customer Information"), and shall make no use of it. To this end, the banking corporation shall implement technological solutions to support the confidentiality and protection of their customers' information, and provide an audit trail on attempts to access information, including information on means to access the accounts of the other corporations.

(c) Notwithstanding Section (b) above, a banking corporation may use customer information provided it has obtained the customer's explicit approval to do so and that the information shall be provided to the customer only.

(d) A banking corporation shall activate the Service only at the customer's initiative and after the customer has given his consent thereto.

(e) A banking corporation shall delete from the relevant databases the information allowing access to the accounts of a customer requesting to unsubscribe from the Service.

(f) A banking corporation shall not condition the provision of the Service on obtaining the customer's consent as prescribed under Section (c) above.

Chapter H1: Transferring Information Regarding the Balance in a Current Account

73a. If a banking corporation's customer requests that information regarding the balance in the customer's current account at the banking corporation be sent to a financial entity, in order to be provided credit, the requested information shall be provided, and the following provisions shall apply:

(1) The customer's request is to be submitted to the banking corporation through E-Banking services that are agreed upon by the banking corporation and the customer for the purpose of executing transactions, or through the customer's request at the branch of the banking corporation. The request is to be documented by the banking corporation.

(2) The customer's request is to note the details of the financial entity to which the customer wants to transfer the information, as well as the frequency of the transfer of information, the period during which the information will be transferred, and the details of the contract with the financial entity in order to transfer the information.

(3) The banking corporation shall enable the customer to choose the frequency at which the information is transferred, from among the following four options: daily, every 3 days, weekly, or monthly.

(4) The banking corporation shall send a notice, through one or more E-Banking channels, and if that is not possible, via mail, to all customers that did not submit such a request on their own to the banking corporation. The notice is to include all the relevant details required for the customer, including the name of the financial entity to which the customer requested to transfer the information, the frequency at which the information is to be transferred, the period of the authorization, and the ways available to the customer for approving the request for the banking corporation. In a corporate account, the banking corporation shall act in accordance with the corporation's decision as it is presented to the banking corporation.

(5) A request to transfer information regarding the balance, as requested by the customer, shall be executed no later than 3 business days from the date of receiving the authorization of all the account holders, provided that the financial entity previously arranged the interface with the banking corporation, in accordance with the format established in Subsection 8 below. Arranging the interface with the banking corporation shall take up to 14 business days from the fulfilling of the financial entity's undertaking to set up its side of the interface. The banking corporation shall notify all the account holders in writing of the carrying out of the request, and any changes in it, and provide the details.

(6) Information regarding the balance in the customer's current account shall be transferred, and it is to be updated to the end of the business day preceding the transfer date. In addition, the following details are to be submitted as well in order to transfer the information: the customer's Israeli ID number (or passport number, for a nonresident), customer's account details—account number, branch and bank, date to which the balance is updated, currency.

(7) The customer shall be permitted to cancel the request at any time via notice to the banking corporation, in a manner listed in Subsection 1 above, and the cancellation shall go into effect no later than 3 business days after receipt of the cancellation request at the banking corporation.

(8) The information shall be transferred from the banking corporation to the financial entity in the format detailed in Appendix C, through a virtual vault or any other secured manner agreed upon by the banking corporation and the financial entity.

(9) A banking corporation that requests to verify that the financial entity is supervised under the law and regulation as an issuer or as a credit provider, may do this through updated publications on the websites of the organizations supervising such entities.

In this Section and in Appendix C, "Financial Entity"—as it is defined in Section 1 of the Banking (Service to Customer) Law, and that is supervised under the law or regulation with regard to its financial activity as an issuer or credit provider as established in Section 7e.(c) of the Banking (Service to Customer) Law.

Chapter I: Reports and Approvals

Issues requiring reporting

74. Canceled.

Issues requiring approval

75. A banking corporation wishing to carry out a significant new E-Banking activity in the banking system in Israel, which is submitted for the approval of the bank's Board of Directors, shall contact the Banking Supervision Department, presenting an analysis of all the risks and means of managing them, to obtain the approval of the Banking Supervision Department thereof.

76. A banking corporation wishing to implement technology for remote face to face identification and authentication in order to open online accounts or to offer its customers account aggregation services shall notify the Banking Supervision Department in advance, presenting all the risks and means of managing them, to receive the approval of the Banking Supervision Department thereof.

Chapter J: Transitional provisions

77. A customer who signed an agreement with a banking corporation for receiving information and carrying out transactions via fax prior to the date of implementing Amendment 7 to the Directive in this regard, shall not be required to sign an agreement for providing e-banking service in this regard via fax, as noted in Section 28 of the Directive, and the requirement in Section 32 above shall not apply with regard to these agreements.

*** * ***

Updates

Circular no. 06	Version	Details	Date
2507	**1**	**Original circular**	**July 21, 2016**
2529	**2**	**Update**	**March 6, 2017**
2547	**3**	**Update**	**December 25, 2017**
2557	**4**	**Update**	**March 22, 2018**
2570	**5**	**Update**	**October 4, 2018**
2578	**6**	**Update**	**November 13, 2018**
2588	**7**	**Update**	**May 7, 2019**
2599	**8**	**Update**	**December 29, 2019**
2645	**9**	**Update**	**December 29, 2020**
2667	**10**	**Update**	**July 25, 2021**
2669	**11**	**Update**	**September 30, 2021**

Appendix A - Signing up Remotely for E-Banking Services: Extensions to Additional Cases

Cancelled.

Appendix B - Opening and Managing a Long-Term Savings Account for a Child

Cancelled.

Appendix C – File Format for Transferring Information on Customer's Balance in a Current Account

In accordance with the provisions of Section 73a(8) of the Directive, the banking corporation is to transfer to the financial entity a file in CSV format with the following structure (the field type and length appear in parentheses):

1. Complete bank number (numeric, 2), branch number (numeric, 3), account number (numeric, 10), customer's Israeli ID number or passport number for a nonresident (alphanumeric, 20), balance (alphanumeric, 17)13 digits to the left of the decimal point, 1 field to mark the decimal point, 2 digits to the right of the decimal point for agorot (100 agorot=1 NIS), another field to mark the balance "+/–"]), date of update of the balance using format YYYYMMDD (numeric, 8), currency (alphanumeric, 3).
2. The fields are to be separated by a semicolon (;). Every line in the file shall represent the record for a specific customer for a specific account.
3. The file name is to be: BALANCE_BBBBB_YYYYMMDD, where:
   BBBBB—represents the bank number
   YYYYMMDD—represents the day that the file was sent.