Bank of Israel
Banking Supervision Department
Policy and Regulation Division

15 Tamuz, 5776

July 21, 2016

Circular no. C-06-2507

Attn:
The banking corporations and the credit card companies

Re: E-banking
(Proper Conduct of Banking Business Directive No. 367)

General

1. In recent years there has been marked growth in the extent of bank customers' use of e-banking services. Alongside growth in the extent of use, banking corporations feel the need to consistently and rapidly update banking products and services—due to customers' expectations, the rapid development of technology, and the increasing competition from fintech companies offering various banking services.

2. The publication of a dedicated directive on the issue of e-banking emphasizes the importance that the Banking Supervision Department places on continued development of digital banking, and this is in order, in addition to the reasons noted above, to support the processes to increase efficiency that are required of them.

3. The goal of the directive is to remove existing barriers to continued development of digital banking and to provide flexibility with regard to the changing technology, without the banking corporations having to turn to the Banking Supervision Department about every change in, or addition to, of a service, so long as they are not material changes or additions. Therefore, the Directive is structured mainly on principles, as well as specific guidelines where the Banking Supervision Department felt that it was required. A principles-based approach places increased responsibility on the banking corporations, and requires them to act with the necessary caution and to constantly improve the existing framework for risk management and to adopt it to the dynamic technological environment in which they operate.

4. It is the Banking Supervision Department's intention to publish additional directives in the future that will complete the required risk-management framework.

5. After consulting with the Advisory Committee on Banking Matters and with the approval of the Governor, I have established the following Proper Conduct of Banking Business Directive, as detailed below.

Structure of the Directive

6. The Directive consists of nine chapters:

   a. **Chapter A: General** – Introduction, applicability, and definitions

   b. **Chapter B: Corporate governance** – details the functions of the board of directors and senior management

   c. **Chapter C: Opening an online account and signing up for E-banking services** – deals with opening an online account, the agreement for providing E-banking services, signing up for e-banking services remotely, and concluding an agreement remotely.

   d. **Chapter D: Identification and authentication** – details the required principles on the issue of identification and authentication.

   e. **Chapter E: Protection of customers** – Deals with training customers using e-banking services and the controls implemented by the banking corporation to protect the customers, such asmonitoring exceptions and sending alerts of atypical activity, and on transactions in accordance with the banking corporation's judgment.

   f. **Chapter F: E-banking controls** – Deals with controls integrated into certain activities, including: Updating account information, executing transfers and payments, and securing the communication between the customer and the banking corporation via e-banking channels.

   g. **Chapter G: Controls for specific channels and devices** – Deals with controls that the banking corporation is to implement in specific channels and devices used for e-banking, such as email, mobile devices, and automated self-service machines.

   h. **Chapter H: Account aggregation** – Details the principles that the banking corporation is to implement when it aggregates information for customers

   i. **Chapter I: Reports and approvals** – Details the reports required on the issue of e-banking and situations in which it will be required to contact the Banking Supervision Department in order to receive approval for a new activity.

Details by sections

Chapter A—General

Introduction (Sections 1–6 of the Directive)

7. The Directive regulates the banking corporations' e-banking activity vis-à-vis their customers and allows remote activity in a range of banking services, so that the customer can receive service in any place, and at any time.

8. The Directive establishes principles for managing the risks in e-banking, both in the banking corporation's internal systems and processes and in conduct vis-à-vis the customer through training and increased awareness of the risks inherent in activity, and in the realization of risks. The Directive establishes a range of controls that the banking corporation is to implement in order to minimize the risks generated by e-banking activity, which is expected to continue and expand to a larger number of customers and to a wider range of channels and services.

9. The framework required in the Directive for managing the risks in e-banking is part of the overall framework at a banking corporation for managing risks, anchored 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" as well as technological and other aspects in various directives, including Proper Conduct of Banking Business Directive no. 357 on "Information Technology Management" while coordinating with Directive 357 including its Section 3(b), as well as various aspects of Proper Conduct of Banking Business Directive no. 361 on "Cyber Defense Management". It should be clarified that the reference to these and other directives does not impose those directives on banking corporations to which those directives do not apply.

Applicability (Section 7 of the Directive)

10. The application of the directive to e-banking is in accordance with the application of Proper Conduct of Banking Business Directive no. 357, including an acquirer as defined in Section 36(i) of the Banking (Licensing) Law, 5741-1981.

Definitions (Section 8 of the Directive)

11. The definitions are intended to clarify the framework for implementing the Directive and to allow a uniform language and coordination of expectations. Thus, definitions were set for "e-banking services" and "authentication factor", which are used throughout the Directive as a central component in the control framework.

12. Automated self-service machines—stands for self-service posts, excluding those which are not automated.

Chapter B—Corporate governance

Board of directors (Sections 9–12)

13. The Directive details the board's areas of responsibility, including the responsibility for verifying that the risks embodied in e-banking, including information security risks, fraud and embezzlement risks, legal risks, and reputational risks, are managed appropriately and in accordance with the existing risk-management framework.

14. The board is to review and approve a risk management framework for e-banking to be anchored in a policy paper. The policy is to include, among other things, principles and parameters for classifying e-banking transactions by risk level, on the basis of which the mandatory means of identification and authentication shall be determined. The policy document is to be integrated into the existing policy documents that serve as part of the overall risk management framework.

Senior management (Sections 13–17)

15. Senior management is responsible for formulating and instilling the policy, setting clear areas of responsibility, allocating appropriate resources for risk management and also for supervising the implementation of the framework for managing e-banking risks.

16. The Directive imposes on senior management the responsibility for defining a plan for taking ongoing actions and to increase customers' awareness of the risks

inherent in e-banking, with the view that the customer's alertness is important in minimizing risks.

Chapter C— Opening an online account and signing up for e-banking services

Opening and managing an online account (Sections 18–27)

17. The Directive makes it possible to open an account online for a new or current customer in a manner similar to the process allowed in Directive 418 on "Opening accounts via the Internet", which is cancelled in the framework of this Circular.

18. The process of identification and authentication is similar to that required in Directive 418 (Sections 18 and 21).

19. To remove doubt, issuing a credit card under the conditions established in Section 6a(a)(2) 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 is not included in the opening of an online account as noted in Sections 18–27 of the Directive.

20. At this stage, in light of the signature requirement in the Debit Cards Law, 5746-1986, reaching an agreement for the issuing of a payment card cannot be concluded online.

21. In carrying out a "Know Your Customer" process (Section 22), a transfer will be allowed from the banking corporation in which the account was opened to an account under the customer's name in another banking corporation in Israel, with receipt of a report from the customer on the precise amount received, and not just a transfer from an existing to the new account, as was the case until now.

22. We clarify that at the point of opening an account pursuant to this Section, the banking corporation shall be permitted to sign up the customer for e-banking services within the framework of an agreement to open an account, and then the relevant sections of the Directive will apply.

Agreement to provide E-Banking services (Sections 28–32)

23. It is emphasized that the Banking Supervision Department views an agreement to provide e-banking services as part of a general terms of business agreement or an agreement to open and manage a current account as noted in Sections 3(a)(1) and 3(a)(2) of the Banking (Service to Customer)(Full disclosure and submission of documents) Rules, 5752-1992, and therefore this Directive does not derogate from the requirement established in the rules, according to which the agreement is to be in writing and the customer is to be able to review it before agreeing to it.

24. An agreement to provide e-banking services will enable a customer to choose separately each channel and each service as defined by the banking corporation. The banking corporation may also define a group of services or group of channels. In this regard, a group of channels means one or more channels necessary for supporting a service. Likewise, the banking corporation is to notify the customer of the risks inherent in the use of e-banking services before giving the customer the option of certifying that he or she read the agreement.

    It is clarified that a customer who signed an agreement to provide e-banking services for receiving certain services through certain channels in accordance with

Section 20 of Proper Conduct of Banking Business Directive no. 357, shall not be required to again sign an agreement to provide e-banking services based on this Directive for the same services through the same channels.

It is emphasized that it is important for there to be an updated presentation of the range of services and channels that the customer has chosen to join, available at any time.

25. A customer that signed an agreement regarding telephone instructions as noted in Section 3(a)(9) of the Full Disclosure Rules, shall not be required to sign an agreement to provide e-banking services regarding receiving instructions to execute transactions by telephone in accordance with this Directive. In this regard, it is clarified that a telephone-instruction agreement can be part of an account-opening agreement, general terms of business agreement, or issuance agreement.

26. It is clarified that all the services carried out through automated self-service machines require an agreement to provide e-banking services. However, if services were given to someone who does not have an account at the banking corporation to which the automated self-service machine belongs, there is no requirement for an agreement. For example, a customer of Bank A can withdraw money from an automated self-service machine of Bank B, even without holding an account at Bank B so that the customer has not signed with it an agreement to provide e-banking services.

Signing up for e-banking services remotely (Sections 33–38)

27. The Directive enables a banking corporation to remotely sign up for e-banking services, for all types of services and channels, customers who have already opened an account.

28. The Directive refers to the identification procedures required in various cases as well as to controls for authenticating the person carrying out the transaction.

29. A customer that requests to remotely sign up, for the first time, to e-banking services, and does not yet have sufficient means of authentication to remotely verify his identity, is required to go through an authentication process, similar to that required when opening an account online (Sections 35 and 36).

30. When signing up for e-banking services solely to receive information or when adding a channel solely to receive information, authentication based on at least one factor is required, and when a customer does not have an authentication factor, use of identification particulars listed in the account must be used, as well as the combination of several questions that make authentication possible (such as account activity, standing orders, automatic salary deposits, and dates of charges).

31. When signing up for a channel to carry out transactions or when joining a service that includes carrying out transactions, whether through the service being signed up for through signing up for another channel to which the customer subscribes, identification through at least two authentication factors out of the authentication factors appearing in the definition is required.

32. The Directive adds to the issue of terminating the contract for e-banking services and establishes that the identification and authentication are to be made at the same identification and authentication levels established by the banking corporation for ongoing use of the service.

Establishing an agreement remotely (Section 39 of the Directive)

33. The Section details guidelines for the remote setting up of agreements that are not legally obligatory for signing up the customer in writing. Among other things, it is established that the banking corporation is to operate a means that will ensure that the customer confirms that he was given the opportunity to read the agreement and agreed with its terms.

34. The banking corporation is to enable the customer to look over the agreement at any time in clear and readable manner, and be able to print it.

Chapter D—Identification and Authentication

Identification and Authentication (Sections 40–44)

35. The chapter deals with identification and authentication of customers in e-banking activities.

36. A banking corporation is to establish means of personal identification and authentication in accordance with the risk assessment and policy approved by the board of directors.

37. A banking corporation is to institutionalize processes to deal with the means of identification and authentication, beginning from the stage they are set up and transferred through the stage of operation and switchover. When transferring means of identification to the customer, the banking corporation is required to verify that sensitive data is not exposed.

38. Managing the means of identification and authentication, including the passwords, shall be the responsibility of the banking corporation and subject to adequate risk management. The Directive does not include specific guidelines regarding changing passwords, their release, or manner of switching them and leaves it to the banking corporations' full judgment. With that, it should be clarified that one authentication factor (such as OTP) alone may not be relied upon for recreating another authentication factor (such as permanent password) and thus create 2 authentication factors by means of one authentication factor.

39. Section 42 details a list of high-risk activities that require use of at least two-factor authentication (2FA). This list is not exhaustive and the responsibility for determining high-risk activity is the banking corporation's as noted above.

40. An account for which several account holders are listed and that requires the agreement of all the account holders to carry out a transaction (in accordance with regulatory directives, agreement, or an inclusive account) will require the agreement of all account holders in the execution of e-banking activities as well (Section 43). In a corporate account, one function will be able to act alone, even if the account holders' consent is required, after receiving verified approval from an authorized entity at the corporation (Section 44).

Chapter E—Protection of customers

Monitoring exceptions and high-risk transactions (Sections 45–47)

41. The growth in e-banking activities raises concern of an increase in risks of fraud and embezzlement. As such, banking corporations are required to expand and increase the sophistication of the mechanism for monitoring anomalies in customers' accounts as well as in activities that are not anomalous but are defined

as high-risk, including, but not limited to, the activities classified as such in Section 42 of the Directive.

42. In addition, the monitoring mechanism is to be updated in line with the methods of fraud and threats to e-banking that are exposed in Israel and worldwide.

Alerts to customers (Sections 48–51)

43. A banking corporation is to make use of anomaly monitoring in order to alert customers to the extent necessary and to take immediate measures such as the suspension of a transaction or of obtaining the customer's approval for a transaction before it is executed. Likewise, the banking corporation will consider in accordance with its risk assessment, the delivery of alerts on various transactions in the customer's account, such as transfers above a set threshold, change of password, change of contact information.

44. The banking corporation is to use communication channels in order to alert as rapidly as possible taking into account the level of sensitivity or risk of the transaction. It is plausible that much use will be made of SMSs due to the extensive use of mobile phones and the speed with which the alert travels, but the banking corporation is to use other channels when sending an SMS is not possible or in accordance with the customer's request.

45. In an account that has several account holders, an alert is also to be sent to the other account holders so that they will serve as an additional control on the account.

Customer guidance (Sections 52–55)

46. In view of the risks inherent in e-banking activity, the banking corporations are required to take measures in order to clarify to customers the substantiality (in addition to the requirement to present the risks before approving the agreement), and thus, to train customers how to protect themselves from such risks and to guide them on the measures to take to minimize them both in terms of behavior and in terms of technology (including installing software or components on mobile devices). The training can also be given through a range of digital channels as well as in branches.

47. The banking corporation is required to manage the inherent risk of phishing or any other fraud or scam that is liable to cause customers to divulge, either on purpose or accidentally, confidential information such as means of identification and authentication. In exceptional cases where there is suspicion of said suspicion, such as, for example, fraud that may affect numerous customers in a short time frame, the banking corporation shall notify its customers who are at risk.

Chapter F—E-banking controls

Updating of account information (Sections 57–59)

48. Updating contact details or updating the name of the account holder are activities that are considered high risk and therefore their authentication level is at least 2FA. Likewise, the banking corporation is to carry out heightened monitoring (such as stricter thresholds for monitoring) of accounts in which an atypical activity was carried out which relates to remote updating of account details (such as:

simultaneously updating several details), for a period of time to be set by the banking corporation and in accordance with the risk assessment.

Transfers, payments, and other transactions (Sections 60–62)

49. In transfers and payments to beneficiaries, the banking corporations are to establish two thresholds for carrying out transactions: the first threshold for which 2FA will be required, and a second threshold above which will obligate the use of technology combing identification and authentication, confidentiality and completeness of data and prevention of denial. We emphasize that the definition of a beneficiary in this Directive does not include a beneficiary located in accordance with Proper Conduct of Banking Business Directive no. 439.

50. The thresholds could be determined individually or by groups of customers or types of beneficiaries while taking into account information technology considerations.

Securing communication channels (Sections 63–65)

51. When a banking corporation receives information that is subject to a confidentiality obligation from customers, or transmits said data to its customers, it is obligated to use an encrypting algorithm in order to protect the data being transmitted over external networks, including the Internet.

52. Encryption shall not be required when transmitting alerts to customers as required by this Directive and when transmitting data by email related to the account of a foreign bank given the terms detailed in the Directive.

Chapter G—Controls for specific channels and devices

Customers' activity via email (Section 66)

53. Notwithstanding the provisions of the "Securing communication channels" section, when receiving data from a customer via email, the banking corporation is to consider the need for encryption and installing additional information-security controls, in accordance with the risk assessment.

Short Messages Services (SMS) (Section 67)

54. As an encryption algorithm cannot be used when sending text messages, full identifying details of customers and their accounts are not to be included when sending information through this channel.

Use of mobile devices (Sections 68–70)

55. An increase in the use of mobile devices—particularly mobile phones—for remote communication requires banks to assess the specific risks they incorporate, and to examine the implementation of processes and controls to minimize the risks. For example, a banking corporation is to take into account aspects of physical security of devices, including locking or installing protective software, as well as handling theft or loss including cancellation of its use for certain transactions, in particular for sending alerts and OTP. The banking corporation shall publish the telephone number for reporting a loss or stolen device.

56. Among the processes that can be implemented, a banking corporation shall consider recording the mobile devices that are used and recording identifying details of the device, which will allow its identification when used to carry out a transaction.

Automated Teller Machines (ATM) (Section 71)

57. A banking corporation shall implement controls in automated self-service stands, to prevent fraud and embezzlement. The controls include support for smart cards (as per the understanding in Proper Conduct of Banking Business Directive no. 470 on "Debit Cards",) and installing a control route.

Instructions for performing transactions via telephone by human response (Section 72)

58. This section is based on Proper Conduct of Banking Business Directive no. 435 on the issue of "Telephone instructions" and is integrated into the Directive in view of the cancellation of Proper Conduct of Banking Business Directive no. 435.

Chapter H—Account aggregation (Section 73)

59. Rules for providing account aggregation services were set. The conditions set by the Directive for a banking corporation to offer account aggregation services were intended, among other things, to maintain the confidentiality of the customer's information, and to regulate the use of the customer's information from other banking corporations.

60. Among other things, it was set that a banking corporation is to implement means of protection against the use of such information. The intention is to ensure that a banking corporation, whether through technology or through its employees, shall not approach and shall not make use of the customer's information that is received from other banking corporations, unless it received explicit approval from the customer to do so, and this is in order to offer value to the customer with regard to all his or her accounts and that the information shall be transferred solely to the knowledge of the customer.

61. It should be noted that the limitation written in Section 17 (c) of Proper Conduct of Banking Business no. 357 was deleted, and from now on outsourcing of account aggregation services will be allowed, subject to the approval of the Banking Supervision Department.

Chapter I—Reports and approvals (Sections 74–76)

Issues requiring reporting

62. Activities regarding which there is an obligation to report to the Supervisor of Banks or to receive the Supervisor's approval were established.

63. Issues requiring reporting include atypical events related to e-banking activity for which there is concern of the materialization of a risk liable to impact on a large number of customers in a small period of time, such as: the discovery of a site for phishing or other fraud, as well substantial attempts at penetration and actual penetrations that are liable to cause a stop in activity.

Issues requiring approval

64. Issues that require the Supervisor's approval include substantial new technological activity that is brought to the board for approval. For other issues, the Banking Supervision Department expects that when there is a doubt about the need to contact the Supervisor, the banking corporation will consult with the Banking Supervision Department a reasonable amount of time prior to beginning the new activity. In any case, the Banking Supervision Department's consent will be required to offer account aggregation services. Contact with the Banking Supervision Department is to be made at least 60 days prior to the beginning of the new activity.

Other issues

Cancellation of existing directives and authorizations

65. Beginning with the date of the start of this Directive, the following directives and authorizations will be cancelled:

    (a) Proper Conduct of Banking Business Directive no. 357 "Information Technology Management", Sections 3(b)(5), 13(a), 13(a1), 17(c), 19–28, 30(a)(1), (1b), and (4), and 30(b)(5) and (6).

    (b) The authorizations given by the Supervisor of Banks or someone on the Supervisor's behalf in accordance with Section 30 of Directive 357 and that relate to the Sections cancelled above, except for authorizations granted for account aggregation services. To the extent that a banking corporation holds an authorization that permits an activity that does not meet the guidelines of this directive, the corporation is to notify the Supervisor of Banks in order to clarify the issue.

    (c) Proper Conduct of Banking Business Directive no. 418 on "Opening of bank accounts via the Internet".

    (d) Proper Conduct of Banking Business Directive no. 435 "Telephone instructions".

    Likewise, beginning with the date of the start of this Directive, the following sections in Proper Conduct of Banking Business Directive no. 357 are to be updated:

    (e) Subsection (e) is to be added to Section 12: "Notwithstanding the provisions of Sections (a)–(c) above, customers using e-banking services as defined in Proper Conduct of Banking Business Directive no. 367 on "E-banking shall be subject to the relevant sections in that directive".

    (f) The following words are to be added to Section 14(b)(2): "As detailed in Proper Conduct of Banking Business Directive no. 367".

    (g) The following references are to be deleted from Section 29(e): "21, 22, 23, 24, 25, 26, 27(c), 27(d)(1)(c), 27(d)(1)(d), 27(d)(1)(e), 28". In their place, the following words should be added: "and to comply with Proper Conduct of Banking Business Directive no. 367".

    (h) Subsection (e) is to be added to Section 30: "Notwithstanding the provisions of Sections (b), (c), and (d) above, in regard to reporting on an event or suspicion of an event of deception in e-banking services and in regard to a

significant occurrence related to e-banking including substantial attempts of penetration and actual penetration, cessation of system services and frauds in e-banking service systems, the reporting provisions detailed in Proper Conduct of Banking Business Directive no. 367 on "E-banking" shall apply".

Start

66. The provisions listed in the Directive pursuant to this Circular will go into effect beginning on 1.1.2017, except for Section 71(b) (Functional support for carrying out transactions via a smart card at automated self-service machines), which will go into effect on 1.1.2018.

67. A banking corporation may act in accordance with this directive at an earlier date than the one set in Section 66 above, provided that Section 65 above applies to it from the same date.

68. If a corporation chose to act as noted in Section 67 above, it shall notify the Supervisor of Banks 30 days prior to said date.

Revised file

69. Update pages for the Proper Conduct of Banking Business Directive file are attached. Following are the provisions of the update:

Insert page	**Remove page**
(07/16) [7] 357-1-14	(4/12) [6] 357-1-20
(07/16) [1] 367-1-14	
	(2/16)[2] 418-1-3
	(1/15) [3] 435-1

Respectfully,

Dr. Hedva Ber

Supervisor of Banks