**Bank of Israel**
Banking Supervision Department
Technology and Innovation Division
IT Regulation and Examination Unit

Jerusalem, March 22, 2018
**Circular no. C-06-2557**

Attn:
**Banking corporations and credit-card companies**

**Re: E-Banking**

(Proper Conduct of Banking Business Directives nos. 367 and 420)

## Introduction

### Opening an online account

1. In view of technological progress in the field of remote face-to-face identification and authentication, and the desire to maximally simplify the identification and authentication process in opening an online account, and making such an account as similar in characteristics as possible, and/or as needed, to an account opened in the conventional manner—all of which subject to appropriate controls—we wish to update the guidelines put forward in the Directive for the opening and management of an online account. The principal changes follow:

   - Allowing the possibility of opening an online account using any face to face identification and authentication technology that satisfies the principles in the Directive, including technology that does not entail real-time interaction with the customer with the exception of special cases that the Directive specifies as requiring such interaction. It should be emphasized that it still remains possible to identify and authenticate an online-account applicant in the manner practiced thus far, i.e., by a combination of videoconferencing technology, use of an ID card and an additional identifying document, and a bank transfer.

   - Extending the possibility of opening an online account to persons who do not have a bank account, by eliminating the need to make a bank transfer to/from an existing bank account as a condition for opening an online account. This option is relevant for banking corporations that elect to use a remote face-to-face identification and authentication technology that satisfies the principles put forward in the Directive.

   - Eliminating the need to present an identifying document in addition to an ID card for banking corporations that elect to use a remote face-to-face identification and authentication technology that satisfies the principles put forward in the Directive.

   - Henceforth, a minor who has reached the age of 16 may also open an online account.

   - Eliminating the need for a bank transfer in the process of opening an online loan account, and this, for loans of up to NIS 50,000.

- Eliminating the need to use videoconferencing technology in an acquiring account opened online, in which annual acquiring volume does not exceed NIS 50,000, and allowing a business to begin using such an account even before a bank transfer is made.

2. In addition to the changes pertaining to the contents of the "Opening and Managing an Online Account" chapter, as stated above, the structure and sections of the chapter have been updated in order to reflect more accurately the sequence of actions in the process of opening an online account.

**Choosing a channel for the delivery of alerts to customers**

3. Even if a customer chooses a specific channel or instrument with which to receive alerts and request authorizations as set forth in Section 50 of the Directive, a banking corporation may, in certain cases of need to contact the customer in real time after suspicious activity in the account has been detected, approach the customer via an additional channel of its choosing. The purpose of this amendment is to give the customer added protection in the event of irregular activity in his or her account.

**Email activity**

4. In view of inquiries from banking corporations and to create an additional possibility of regular communication between a banking corporation and a customer under certain conditions, the Directive has been amended to allow banking corporations to send customers information by email without encryption, subject to an appropriate risk assessment and additional controls as specified in the Directive and in the explanatory remarks. It is stated for clarity, however, that if an alternative way to perform the transactions on the banking corporation's site exists, this method of performing the transactions is preferred.

**Amendments to the Directive**

**Opening an online account**

5. The online-account applicant shall be an individual resident of Israel who is at least 16 years of age **(Section 18(a) of Directive 367)**.

   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: "minor") shall be subject to the following stipulations:

   (1) The process of opening an account for a minor, including identifying and authenticating the minor in accordance with Section 19 below, the "Know Your Customer" process, and a declaration on account beneficiaries, shall be conducted remotely through a face to face interaction in real time with a banking corporation representative. During the course of the process of opening an account for said minor, the banking corporation shall provide a face-to-face explanation to the minor with 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

**(Section 18(d) of Directive 367)**

**Explanatory remarks**

The amendment to the Directive extends the right to open an account under the provisions of Proper Conduct of Banking Business Directive 416, "Minors' Accounts" (hereinafter, "Directive 416") to minors who have reached the age of 16. Insofar as a banking corporation chooses to identify the minor and authenticate his or her identity in the manner specified in Section 19(a) of the Directive, the minor will not have to have an account with the banking corporation at the time he or she opens the online account.

When an account is opened for a minor, certain aspects come to play that are different from the characteristics of an ordinary account. The amendment to the Directive allows a minor to open an online account in a process, and with the characteristics, that resemble as closely as possible those of an account opened in the conventional manner. For this purpose, the following instructions, *inter alia,* are set forth:

5.1 Since this is the first encounter with a banking corporation for most minors, and since in the account-opening process the minor may have various questions about the characteristics of an account and the principles for managing one, the banking corporation shall, as part of the account-opening process:

- maintain real-time interaction between one of its representatives and the minor so that the minor may receive immediate explanations for questions that he or she may ask in regard to the account, the process of opening the account, and the management of the account, all of which similar to what minors who wish to open an account at a branch may do today. It should be emphasized that even a banking corporation that uses remote identification and authentication technology as determined in Section 27a of the Directive must use a technology that allows real-time interaction with one of its representatives when an account is being opened for a minor.

- explain to the minor, using face-to-face instructional aids (such as a video clip) or by means of the banking corporation's representative in real time, the principles of managing a bank account, with emphasis on the special characteristics of a minor's account (in regard to which, see Directive 416). It shall be emphasized that said aids and explanations by a representative of the bank in real time shall not be considered a substitute for the banking corporation's duty under Section 16 of Directive 416 to present the minor with an information sheet that spells out his or her obligations and rights and provides full details about the fees and other charges that may pertain to the account.

5.2 A representative of a minor who wishes to open an overdraft account and obtain a credit card shall sign, at the branch, an appropriate written statement of permission as set forth in Directive 416. To offer the same options to a minor who applies to open an online account, a banking corporation shall allow the minor's representative to identify him or herself online for the purpose of giving said permission.

Face-to-face identification and authentication of the minor's representatives shall take place in accordance with one of two alternatives set forth in Section 19 of this Directive and may be carried out either as part of the process of face-to-face identification and authentication of the minor him/herself or independently thereof. In any case, the bank shall authenticate the relationship between the minor and the representative of the minor in the manner by which it authenticates said relationship for an account opened at a branch, e.g., by means of the stub of the representative's ID card on which his or her children's particulars are recorded. Notably, for a banking corporation to rely on a document for the purpose of authenticating the relationship between the representative and a minor, it must authenticate, *inter alia,* the originality of the document even when this is done online. If the banking corporation chooses the option of using remote face-to-face identification and authentication technology to identify the account-opening applicant, it must verify the originality of said document by means of the same technology.

Notably, for the time being it is not be possible to obtain the consent of a minor's representative for investing the minor's funds in any investment vehicle that poses a risk to the principal (Section 15 of Directive 416) by means of said technology.

6. The banking corporation shall digitally document all the face to face identification and authentication processes regarding the online-account applicant, 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, 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". **(Section 18(e) of Directive 367).**

**Explanatory remarks**

Section 7 of the Prohibition on Money Laundering Order, 5661-2001 (hereinafter: "the Order") requires banking corporation to retain "identification documents", as defined in the Order, for a period of at least seven years after the account is closed, or longer if the Supervisor of Banks so requires.

Section 18(e) of the Directive states that when an online account is being opened, all digital documentation of the entire face-to-face identification and authentication process of the account-opening applicant, and of the representative of a minor in case his or her consent is required for there to be an overdraft facility in the minor's account and issuing the minor a credit card; the "Know Your Customer" process that was carried out; the declaration of beneficiaries in the account; and all documents presented within this framework

shall be considered "identification documents" for the purposes of Section 7 of the Order.

7. 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 **(Section 18(f) of Directive 367).**

**Explanatory remarks**

Since Chapter C of the Directive deals with various aspects of identification and authentication when an online account is opened, this Section enables a banking corporation to refuse to open an online account for a customer whom it identifies as being of high risk on line account. It is stated for clarity that "reasonable refusal" is determined in respect of the way the account is opened, i.e., a banking corporation that wishes to invoke this Section must give the customer a physical alternative way to open the account. As for the opening and management of the account per se, this Section neither adds to nor derogates from the provisions of any law.

8. Identification of the online account applicant 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, the following provisions shall apply:

(1) Notwithstanding the provisions of Subsection (b)(1) of this Section, the banking corporation is permitted to not make use of video conferencing technologies.

If the annual acquiring turnover exceeds NIS 50,000, the banking corporation shall establish a threshold until which it will continue to provide acquiring services to

the customer, but will not transfer the acquiring funds that accumulated above NIS 50,000, until the customer completes the identification and authentication process through the use of video conferencing technologies, so long as they have not been used.

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.

(2) The transfer of a random amount to an account at a banking corporation in Israel under the name of the acquiring account applicant, out of the amount of funds that the banking corporation is required to credit the customer the first time that acquiring funds are to be credited, shall be considered as the bank transfer required in accordance with Subsection (b)(2) of this Section.

The provisions of Subsections (a)–(c) above do not derogate from the other obligations detailed in Section 3(a)(1) of the Order. **(Section 19 of Directive 367).**

**Explanatory remarks**

Section 3(a)(1) of the Order mandates authentication of particulars and lists mandatory documents, and Section 6(a) of the Order requires face-to-face identification in one of the ways specified therein. In accordance with the powers of the Supervisor of Banks under Sections 6(a)(5) and 7a of the Order, identifying an account-opening applicant and authenticating the particulars of his or her identity may take place henceforth in one of the following additional ways as well:

(a) Use of technology as specified in the section of this amendment titled "Technology for Remote Face-to-face Identification and Authentication." This technology is meant to identify and authenticate an online-account applicant. It may be implemented via real-time videoconferencing or by video recording that is not in real time, but it must include the relevant controls specified in said chapter.

A banking corporation that elects to use this technology for remote face-to-face identification and authentication may settle for only an ID card for the purposes of the identification and authentication process and shall not demand a bank transfer by means of an account as had been required thus far. The meaning of the amendment is that even a customer who has no bank account can open an account online.

(b) In the manner practiced thus far, i.e., a combination of videoconferencing technology, an ID card, and an additional identifying document, as well as a bank transfer from an account. A banking corporation that chooses this method need not apply the controls set forth in the "Technology for Remote Face-to-face Identification and Authentication" chapter. The use of technology under this alternative is for the videoconferencing requirements only and not for the identification and authentication of the online-account applicant or his or her representative. Said identification and authentication shall be carried out by a representative of the banking corporation. However, the Directive allows the corporation not to fully perform the identification and authentication process set forth under this alternative in two cases:

- If the online account being opened is a loan account in a sum of up to NIS 50,000, a bank transfer shall not be required.

- If the online account being opened is an acquiring account in which the annual acquiring volume is up to NIS 50,000 per year, neither a video conference nor a bank transfer as set forth in this alternative shall be required before the acquiring account is opened. Instead, the banking corporation, after carrying out an appropriate "Know Your Customer" process, may allow the business to begin honoring payment cards immediately. In this case, when the acquiring funds that the business is owed are transferred for the first time, a random sum included in these funds shall be transferred to the bank account of the business and shall be considered a bank transfer. When the customer reports the exact sum received, the banking corporation may immediately transfer the rest of the acquiring funds that belong to the business. If and when the annual acquiring volume exceeds NIS 50,000, the banking corporation will have to complete the identification and authentication process as required by the Directive and shall do so by means of videoconferencing technology. The banking corporation shall also perform a risk assessment concerning the need to carry out an updated "Know Your Customer" process pursuant to the change in the extent of activity in the account.

Irrespective of the alternative that it chooses, the banking corporation shall authenticate the identifying particulars against those in the Population Registry of the Ministry of the Interior and shall compare the date of issue of the document presented to it with the date of issue of the most recent document recorded in the Population Registry, all as set forth in Section 3(a)(1) of the Order.

This Section shall not derogate from the dispensations provided for by the Order in regard to identification and authentication requirements, such as those in Section 6a(a)(2) of the Order.

9. The banking corporation may carry out the "Know Your Customer" procedure via technological means other than those it uses for identification and authentication, provided that 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. **(Section 21 of Directive 367).**

**Explanatory remarks**

A banking corporation need not carry out the "Know Your Customer" process at the same time that it carries out the identification and authentication process for opening an account, and it is not obligated to perform the process using the same technology. The "Know Your Customer" process, for example, may also be performed by means of a telephone call before or after the customer is identified and authenticated and in a manner distinct from this process, provided it take measures to ascertain that the respondent to the "Know Your Customer" questionnaire and the customer identified and authenticated for the opening of the online account are the same person.

10. 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 through the technology that the certificate presented is in fact the certificate of the person identifying themselves, including authentication through comparing the picture on the certificate with the picture of the person identifying themselves via the technology.

(3) Authenticating the details of the person 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) Existence tests

b) Ongoing viewing by a bank representative, with digital documentation that is saved, in order to verify the suitability of the process implemented

(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.

**(Section 27a of Directive 367)**

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.

**(Section 76 of Directive 367)**.

**Explanatory remarks**

It should be emphasized that this procedure shall not apply to a banking corporation that chooses to continue using the method specified in Section 19(b) of this Directive.

The Directive establishes a set of minimum technological controls that should be applied in respect of the customer identification and authentication process. The controls are worded in a general manner so that they will respond, to the extent possible, to future technologies and to additional identification documents that will be approved for use in the future. For the time being, however, it having been determined that the remote identification and authentication process requires an ID card and does not allow the use of any other identifying document (see Section 3(a)(1) of the Order). Therefore, the controls specified in this

Directive shall be implemented in the context of an ID card, be it in a printed version or a biometric one.

The controls specified in the Directive are explained below:

- **Checking of originality of the ID card**—this check may be performed, among other methods, by checking the type of font used in writing it, the positioning of certain fields on the card, and the integrity of the official signature imprinted on the back of the card. It should be noted that, in this matter, the stub of an ID card, which a banking corporation may use when opening an account for a minor in order to authenticate the relationship between the minor and his or her representative, is an integral part of the ID card itself, as Section 25 of the Population Registry Law, 5725-1965, implies.

- **Authenticating through the technology that the certificate presented is in fact the certificate of the person identifying themselves—**this check may be performed, among other methods, by comparing the photograph on the ID card presented with that of the account-opening applicant as documented in the course of the process. Notably, for the time being, a banking corporation must implement this control by photo comparison as stated. However, it is not enjoined against applying this control in additional ways in accordance with the results of its risk assessment. An example, if it becomes possible in the future, is a comparison of the biometric data on the biometric ID card with those presented by the account-opening applicant.

- **Authentication of applicant's particulars on the document presented against relevant databases—**to apply this control, a banking corporation must, at the minimum, check the date on which the ID card was issued with the Population Registry and compare the other identifying details required by the Order with the Population Registry. In the case of an ordinary ID card, this check can be performed, for example, by using Optical Character Recognition (OCR) technology. However, a banking corporation may also carry out this check in additional ways, depending on the results of its risk assessment process, of course.

Insofar as remote face-to-face identification and authentication technology, which obviates the need for real-time interaction with a bank representative, is used, the banking corporation shall also apply the following controls:

- **Existence test—**a check meant to ascertain that the photo presented in the identification and authentication process belongs to a real person and is not the product of some technological manipulation. This check can be performed, for example, by projecting a random sentence onto the account-opening applicant's screen and asking him or her to read it out, confirming thereby that he or she is a real person.

- **Ongoing viewing by a bank representative of digital documentation retained during the identification and authentication process**—because no real-time interaction with a representative of the bank takes place when said technology is used and because the technologies at issue are innovative, a banking-corporation representative should view all digital documentation of every online account that is opened in this manner. The purpose of this requirement is to ensure that the technology has not been abused pursuant to sundry mishaps among other factors.

In addition to the controls, the Directive states that a banking corporation that wishes to use remote face-to-face identification and authentication technology must establish, in advance, minimum technological criteria for the use of this technology. For example, a banking corporation may establish a percentage of Type II errors (false negatives) that it is willing to accept in the course of the identification and authentication process.

Every technology applied for remote face-to-face identification and authentication in opening an online account shall also entail the approval of the Banking Supervision Department. The Department shall be approached at least sixty days before the application of said technology is to begin.

**Choosing a channel for the delivery of alerts to customers**

11. 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. **(Section 50 of Directive 367)**.

    **Explanatory remarks**

    When alerting customers about anomalous activity in accordance with Section 45 of the Directive, a banking corporation may contact the customer using the channel or an instrument of its choosing, even if the customer has specifically elected to receive alerts and request authorizations by means of some other channel or instrument, provided that the channel or instrument in question is not the one in which the anomalous transaction, for which the banking corporation wishes to send the customer an alert, was detected. This, of course, is in addition to sending out the same alert via the channel or instrument through which the customer has asked to have alerts sent to him or her and through which he or she requests authorizations.

    The purpose of the amendment is to augment the customer's protection in the event of anomalous activity as set forth in Section 45 of the Directive and to enable the customer to receive alerts in real time in order to forestall damage when the channel that the customer chose to use is abused by an element that poses a risk and/or in the case of anomalous activity in the customer's account that entails rapid direct contact with the customer.

**Email activity**

12. **Section 64(b) of Directive 367** is repealed.

    **Explanatory remarks**

    In accordance with the change in Section 66 of the Directive (see below), the provisions of this Section (Section 64(b) of the Directive), which makes an exception of the compulsory encryption of email messages that a banking corporation sends to a foreign bank that operates and is supervised outside the borders of Israel, are no longer necessary.

13. 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. **(Section 66 of Directive 367).**

14.(a) Notwithstanding the provisions of Section 63 of Directive 367, a banking corporation may send notices that are not mandated by law without using an encryption algorithm, provided these notices not include full identifying details.

    (b) The provisions of Section (a) above shall not apply to the sending of a notice by email that is subject to the arrangement set forth in Directive 367 **(Section 16 of Directive 420)**.

**Explanatory remarks**

15. The Directive allows banking corporations to carry out a risk-assessment process even for information that they send to their customers and to decide, on its basis, what level of security is needed for each type of information or transaction.

    It is emphasized that a banking corporation that chooses to switch for the first time to unencrypted email transmission to a customer in accordance with the Directive should do so gradually and should make the transition in accordance with the provisions of Section 16 of Proper Conduct of Banking Business Directive 310, "Risk Management," including obtaining authorization from all relevant players at the banking corporation as set forth in Section 16(c) of said Directive.

16. As stated above, a banking corporation shall perform a risk assessment and, in accordance with it, decide on the level of security that shall be applied to each type of information sent by email. It is emphasized that the risk of disclosure of information sent by email that will allow unauthorized elements, including hostile ones, to make inferences about the state of a customer's account over

time and/or about recurring transactions in the account (e.g., when a periodic report about the state of the account is sent out, or when said transmission concerns daily transactions/or balances in a current account over a period of time, or information from which one may infer the customer's regular income and expenses), or that will allow such elements to obtain systemic information about the bank's customers (e.g., when a Webmail server widely used by the bank's customers is hacked or when information on said server is gathered systematically by the email service provider, who may use it for his own needs) shall be considered high-risk, and the banking corporations must apply an appropriate level of security in such cases.

17. The Directive establishes minimum principles for the risk assessment:

- The minimum aspects on the basis of which the risk assessment shall be performed are the following:
  - — type of customer, e.g., retail, commercial, business;
  - — sensitivity and secrecy of the information transmitted;
  - — how frequently the information is transmitted;
  - — the extent of the information;
  - — the estimated level of security of the customer's email service provider, insofar as this can be determined.
- The outcome of the risk assessment shall be a finding about the level of security needed for each type of information or transaction that the banking corporation determines as being allowable for transmission or performance by email.
- The requisite level of security shall determine, among other things, the need for encryption, its strength level, the extent of the need for unequivocal identification of a customer who sends an email message (in the case of a message sent by the customer to the banking corporation) and whether, within the framework of the information sent out, the customer's identifying particulars (e.g., full ID number) or full details of the customer's account (e.g., full account number) may be sent out.

18. In accordance with Section 52 of the Directive, a banking corporation that allows unencrypted transmission of customer information must explain to its customers the main risks of such service and must recommend reasonable security measures when using it.

19. Pursuant to the amendment of the Directive concerning email transmissions from banking corporations to customers, greater use of email-based communication with customers is foreseen. Accordingly, an increase in operating risk, including the risk of customers being defrauded via use of information transmitted, should be expected. Thus, banking corporations must apply appropriate controls, including monitoring, that relate to the various aspects of the matter such as diagnosis, prevention, and handling of information leakage should it be detected. Below are examples of controls that banking corporations should apply when they implement the change in question:

- Technological controls that will prevent transmission of customer information in violation of the rules set forth and by unauthorized staff.

- Technological controls that will quickly issue an alarm about any irregular activity relating to transfer of information in violation of the rules set forth.
- A process that ascertains the currency of the details of the customer's email address.
- Appropriate procedures for cases in which a leak of customer information resulting from erroneous sending of email (e.g., wrong address) is detected.

20. It is stated for clarity that the provisions of Section 66 of this Directive shall not apply to alerts and authorization requests as specified in Sections 48 and 49 of the Directive that are sent by email, to which Section 64 of the Directive shall apply.

21. To complement the amendment of Section 66 of Directive 367 as aforesaid, Section 16 of Directive 420 has been amended. Henceforth, the distinction between a notice issued by force of law and a notice issued not by force of law is immaterial in respect of the level of security, including that of encryption, that shall be required in sending alerts by email. The level of security shall be set in accordance with the risk assessment that the banking corporation shall perform on the basis of the provisions of Section 66 of Directive 367.

**Effect**

22. The amendments to the Directive shall go into effect on the day of their promulgation.

**Revised file**

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

| Remove page | Insert page |
|---|---|
| (12/17) [3]367-1-19 | (03/18) [4] 367-1-19 |
| (01/18) [4]420-1-4 | (03/18) [5] 420-1-4 |

Respectfully,

Dr. Hedva Ber
Supervisor of Banks