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

Jerusalem
December 29, 2020
Circular no. C-06-2643

To:
The banking corporations and credit card companies

Re: Reporting of Technological Failures and Cyber Events
(Proper Conduct of Banking Business 361, 357, 367, 366; Reporting to Banking Supervision Directives 848, 880)

Introduction

1. Rapid technological progress has created opportunities and increased the range of digital services offered to customers. At the same time, it has increased the banks' dependence on this critical infrastructure, and it also has the potential to increase technology and cyber risk. The efficient management and handling of technological failures and cyber events is critical and constitutes a cornerstone in maintaining a bank's functioning and provision of services during such an incident. Accordingly, the Banking Supervision Department has decided to redefine the reporting requirements in these contexts with the goal of ensuring that the banks properly manage the event; in order to obtain an assessment of the situation and to provide assistance if needed; to limit the systemic effect of the event; and to ensure that the process of investigation and lessons learned is implemented appropriately.
2. The obligation of the banks to report to the Banking Supervision Department was until now based on the following directives:
   2.1 Proper Conduct of Banking Business Directive no. 357 on "Information Technology Management" (herein: Directive 357); Proper Conduct of Banking Business Directive no. 367 on "E-Banking" (herein: Directive 367); and Proper Conduct of Banking Business Directive no. 361 on "Cyber Defense Management" (herein: Directive 361) which require that the banks report certain instances of technological failure and cyber events to the Banking Supervision Department.
   2.2 Reporting to the Banking Supervision Department Directive no. 848 on "Reporting of a Cyber Event" specifies how to report a cyber event.
3. In order to achieve greater simplification and efficiency in the reporting of technological failures and cyber events by the banks to the Banking Supervision Department and because in many cases the manner of reporting and management in certain stages of technological failure events is similar to that in the case of a

cyber event, an updating and consolidation has been carried out of the reporting required of the banks according to the directives in order to produce a single unified directive (herein: the Proper Conduct of Banking Business Directive), as well as a new reporting directive.

4. The Proper Conduct of Banking Business Directive defines the requirements for reporting of a technological failure and a cyber event and replaces the reporting requirements that currently exist, as listed in Sections 13–16.
5. After consultation with the Advisory Committee for Banking Business and with the approval of the Governor, I have issued the Proper Conduct of Banking Business Directive and have amended Directive 356, Directive 367 and Directive 361.

Structure of the Directive

6. The Directive includes the following sections:

6.1 General information

6.1.1 **Introduction and goals –** The Proper Conduct of Banking Business Directive specifies the process of reporting to the Banking Supervision Department regarding the management and handling of technological failures and cyber events.

6.1.2 **Applicability –** The Proper Conduct of Banking Business Directive corresponds to the applicability of Directive 357, Directive 367 and Directive 361.

6.1.3 **Definitions –** The Proper Conduct of Banking Business Directive defines the types of events in order to create a uniform reporting language and in order to define expectations. With regard to the reporting of a cyber event, this definition corresponds to the stage described in the definition of "cyber event management" in Proper Conduct of Banking Business Directive no. 361.

6.2 Reporting of a significant technological failure or cyber event:

6.2.1 **Types of events that require reporting –** The Proper Conduct of Banking Business Directive defines the type of events that require reporting to the Banking Supervision Department.

6.2.2 **Responsibility for reporting –** The Proper Conduct of Banking Business Directive defines the responsibility for reporting and the appointment of a Reporting Officer in each bank.

6.2.3 **Manner of reporting –** The Proper Conduct of Banking Business Directive describes the manner of reporting according to the stages of the event: initial reporting of the event, additional reports during the event and reporting the completion of the event.

6.2.4 **Investigation of the event –** The Proper Conduct of Banking Business Directive requires an investigation of the event and learning lessons and the submission of a final report to the Banking Supervision Department.

Points of emphasis

7. The Proper Conduct of Banking Business Directive places emphasis on the reporting of significant events only and therefore the definitions of the types of events to be reported that appear in Section 6 correspond to the Proper Conduct of Banking Business Directive.
8. It should be mentioned that the Banking Supervision Department can change the frequency of reporting according to the nature of the event (either greater or lesser frequency).
9. Manner of reporting
   9.1 A report by telephone will be provided within two hours of identifying the event as one that requires reporting in order to provide the Banking Supervision Department with the initial information required and to facilitate the preparations for handling the event, based on maintaining close contact with the reporting bank.
   9.2 Subsequently, a written initial report will be submitted within 8 hours of the report by telephone in order to give the reporting bank time to get organized and to handle the event and thus to provide a precise and detailed report on the banks. This will facilitate a more focused and efficient handling of the event.
   9.3 As the event develops, an update report is required from the reporting bank on a daily basis or when there is a significant change in the course of the event. This will be done until the completion of the event. The report will include the details known up until the time of the report and they will be cumulative.
   9.4 In the first stage of assimilating the work process according to the Proper Conduct of Banking Business Directive, reports will be submitted by means of the "Kasefet" (virtual vault) system using a spreadsheet file that contains a table structured according to the new reporting directive. In the second stage of the assimilation of the directive, it is the intention of the Banking Supervision Department to install a computerized reporting system that will be used for submitting reports. In exceptional cases, when there is a failure in the reporting mechanism or the classification of the information does not allow it to be submitted by means of the reporting system, the banks will be given instructions for submitting the information by means of an alternative reporting system.
10. In the definition of a "technological failure event", we will further specify that in the case of a severe and widespread effect there are also implications for internal activity, such as: the production systems going down in an active-active mode which activates the backup and as a result service is not disrupted or the severe problem is rectified before there is any actual effect (technological potential as opposed to the potential of a cyber event).
11. When an event is declared as completed by the bank, a qualitative assessment will be carried out by the Banking Supervision Department to confirm that the event is indeed completed.
12. The manner of fulfilling the conditions of the Proper Conduct of Banking Business Directive are described in Reporting Directive to the Banking Supervision

Department 880 on "Reporting of a Technological Failure Event and/or a Cyber Event".

Amendments to the directives

13. **Proper Conduct of Banking Business 357 on "Information Technology Management":**

13.1 "(b) a bank will report the following events and occurrences to the Banking Supervision Department:

(1) A technological failure event according to Proper Conduct of Banking Business 366 on "Reporting of Technological Failure Events and Cyber Events";

(2) Cancelled;"

(Section H: Miscellaneous: Actions that require approval and actions that require reporting: Section 30).

Explanatory remarks:

To be erased: types of events to be reported, instructions for reporting and referral to other directives. A reference to the Proper Conduct of Banking Business Directive was added.

13.2 "(c) Notifications and reports according to Sections 29 and 30 above will be sent to the IT Regulation and Examination Unit within the Banking Supervision Department of the Bank of Israel.

(d) Notifications according to Sections (b)(3) and (4) will be sent 30 days ahead of time.

(e) Cancelled."

(Section H: Miscellaneous: Actions that require approval and actions that require reporting: Section 30).

Explanatory remarks:

The actions that require approval and actions that require reporting which remain in the Directive will be reported directly to the Information Technology Regulation and Examination Unit within the Banking Supervision Department instead of the Information and Reporting Unit.

14. **Proper Conduct of Banking Business 361 "Cyber Defense Management"**

The bank will report a cyber event or an event that is suspected of being a cyber event to the Banking Supervision Department according to Proper Conduct of Banking Business Directive no. 366 on "Reporting of Technological Failure Events and Cyber Events".

(Reporting of a cyber event: Section 82)

Explanatory remarks:

Reports of a cyber event or an event that is suspected of being a cyber event will be made according to the Proper Conduct of Banking Business Directive.

15. **Proper Conduct of Banking Business 367 on "E-Banking**
    Section 74 – cancelled.
    (Section I: Reports and Approvals: Occurrences that need to be reported).

    Explanatory remarks:
    Erased: types of events to be reported, instructions for reporting and referral to other directives (see also Circular C-06-2645).

16. **Proper Conduct of Banking Business 367 on "E-Banking"**
    Reporting Directive 848 will be cancelled.

    Incidence and interim directives
17. This directive and the amendments to the directives will go into effect one month from publication.

Updating of the file
18. Attached are the updates to the Proper Conduct of Banking Business file; following are the updates:

Remove page	Insert page
(11/18) [8] 357-1-15	(12/20) [9] 357-1-14
(3/15) [1] 361-1-19	(12/20) [2] 361-1-19
----	(12/20) [1] 366-1-4

Sincerely,

Yair Avidan
Supervisor of Banks