Bank of Israel
Banking Supervision Department
Technology and Innovation Division
Banking Technology Unit

January 22, 2023
Circular no. C-06-2736

To:
The Banking corporations and credit card companies

Re: Reporting of Technological Failures and Cyber Incidents

(Proper Conduct of Banking Business Directive no. 366)

Introduction

1. The Financial Information Service Law establishes (Section 31.(a) of the law) that "If a severe security incident, as understood in directives pursuant to Section 36 of the Privacy Protection Law, occurs, the service provider shall immediately inform the information source's relevant regulator, the information source from whose information the security incident occurred, and the Registrar, as defined in Section 7 of the Privacy Protection Law (in this section, "the Registrar"), and shall also report to the regulator of the service provider and the Registrar the steps taken due to the incident. If the service provider received the information from a different service provider that collected it, in accordance with the provisions of Section 29(a)(3—it shall immediately notify the service provider from whom the information was obtained as well; if the information source received notice according to this Subsection, it shall report this without delay to the information source's regulator".
2. In order to facilitate reporting by banking corporations on the range of incidents required to be reported to the Banking Supervision Department, and to consolidate such reporting, the Banking Supervision Department determined that the manner of reporting a "severe security incident" to the Banking Supervision Department as the information source's regulator, in the course of a banking corporation's activity as an information source or as a service provider as noted in the law, shall be in accordance with the provisions of Proper Conduct of Banking Business Directive no. 366.
3. This regulation was not accompanied by the publication of a report in accordance with the Principles of Regulation Law, 5782-2021, in view of significant activities that were carried out before the law went into effect, in accordance with the Governor's decision.
4. After consulting with the Advisory Committee on Banking Business Affairs and with the approval of the Governor, I have decided to revise Proper Conduct of Banking Business Directive no. 366 on the issue of "Reporting of Technological Failures and Cyber Incidents".

Changes in Proper Conduct of Banking Business Directive no. 366

5. Section 6.6 was added. It establishes that a severe security incident as understood in Section 31 of the Financial Information Service Law, 5782-2021, that occurs along with the banking corporation's activity as an information source or as a financial information service provider, in accordance with this law, shall also be a type of event that requires reporting to the Banking Supervision Department in a manner detailed in the Directive.

Changes in Reporting to Banking Supervision Directive no. 880

6. In Section 15, "Types of incidents":5—"a severe security incident in accordance with Section 6.6 of Proper Conduct of Banking Business Directive no. 366" was added.

Effective date

The updates to this Directive shall go into effect on the day they are published.

Updating the file

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

Remove page	Insert page
(11/21) [3] 366-1-4	(01/23) [4] 366-1-5

Sincerely,

Yair Avidan
Supervisor of Banks