



October 8, 2018

**Circular no. C-06-2571**

Attn:

**Banking corporations and credit card companies**

**Re: Outsourcing**

(Proper Conduct of Banking Business Directive No. 359A)

**Introduction**

1. In recent years, banking corporations have seen major changes in their activity environment that originate, *inter alia*, in the accelerated pace of technological developments and the adoption of policies meant to enhance competition in banking and payment systems. These changes enable banking corporations to use outsourcing in order to attain strategic goals, make themselves more accessible and available to customers, and pursue continued operational efficiencies. Outsourcing also helps to lower entrance barriers to new and digital players.
2. This Directive specifies the principles that banking corporations must uphold when they outsource various activities. Their purpose is to mitigate the banking corporations' exposure to the potential risks that originate in this form of activity and are based on existing regulations that many countries, such as the United States, Canada, Hong Kong, and Australia, have introduced in recent years, and on a document that a Joint Forum headed by the Basel Committee has published.
3. The Banking Supervision Department is considering the possibility of broadening this Directive to include special points of emphasis in outsourcing technological systems.
4. After consulting with the Advisory Committee on Banking Matters and with the approval of the Governor, I have established Proper Conduct of Banking Business Directive No. 359A on "Outsourcing" (hereinafter, "the Directive").

**Main provisions of the Directive**

**Chapter A—General Remarks**

**Application (Section 7 of the Directive)**

5. Subsection (a) specifies the corporations to which the Directive applies: banking corporations, auxiliary corporations, and corporations controlled by banking corporations as set forth in Sections 11(a)(3a) and 11(a)(3b) of the Banking (Licensing) Law, 5741-1981. The Directive also applies to a merchant acquirer as defined in Section 36(i) of said Law.
6. In Subsection (b) of the Application section, it is emphasized that the Directive shall be implemented within a banking group in a manner that accords with the

existing matrix of relations among the group's constituent companies. For example, a parent company is not expected to perform due diligence for a subsidiary because it analyzes the subsidiary's risk and evaluates its supervision and control mechanisms as part of its own risk-management system, which it applies on a consolidated basis.

7. Subsection (c) allows a banking corporation to apply the Directive *mutatis mutandis* when it contracts with a payment card company as defined in the "Strum Law" and in accordance with the contracting arrangement that said law requires.
8. The Supervision Department shall occasionally consider lenience in applying the Directive vis-à-vis additional statutory entities, such as a "cost comparison service provider" as defined in the Control of Financial Services (Regulated Financial Services) Law, 5776-2016.
9. Subsection (d) allows the Supervisor of Banks to exempt a specific corporation from specific provisions or to determine that other provisions shall apply to it.

## **Definitions**

10. The following definitions were set forth:

**(a) "Outsourcing"**

The definition of outsourcing is meant to explain the cases in which assigning an activity to an outside source will be considered outsourcing for the purpose of implementing the principles of the Directive. According to the definition, outsourcing is an activity included on the list of banking-corporation activities as set forth in Section 10 of the Banking (Licensing) Law, in order to ascertain that it takes place within its business in a way that does not expose it and its customers to unnecessary risks.

Notwithstanding the foregoing, examples of activities that should not be considered outsourcing were added because these are not business activities and do not fall into a banking corporation's area of specialization, e.g., installation of communication infrastructure, and employment of staff via personnel companies. In addition, the Directive states that it should be a "material activity," as defined by the banking corporation, so that it may use discretion in applying the principles of the Directive in accordance with its risk assessment. The level of materiality of an outsourced activity shall be determined by the banking corporation on the basis of the considerations specified in the Directive, *inter alia*.

**(b) "Service provider "**

On the basis of the definition of "outsourcing," a "service provider" is defined as anybody that contracts a banking corporation for the provision of outsourcing services, be it located in Israel or elsewhere.

**(c) "Secondary service provider"**

A "secondary service provider" is defined as anybody who contracts a service provider for the provision of outsourcing services, namely, an entity that contracts with a service provider to perform some or all outsourcing activity under an agreement of the service provider with the banking corporation.

## **Chapter B—Corporate Governance**

### **Board of Directors (Sections 9–12)**

11. Spelled out in this chapter is the responsibility that the Board of Directors assumes when it decides to outsource a given activity. Outsourcing exacerbates various risks because, among other things, it mitigates the effectiveness of the banking corporation's supervision and control of the activity outsourced. Therefore, the Board must ascertain that the banking corporation will continue to honor its obligations, including compliance with all statutory provisions as well as directives of the Supervisor of Banks, its undertakings to its customers, and its responsibility for making sure that the ability of the Supervisor of Banks to discharge h/her duties is not impaired.
12. The Board of Directors must also determine risk appetite and approve a comprehensive policy on the treatment of outsourcing, reapprove it periodically, and approve material contracts. The policy to be approved by the Board of Directors should include guidelines on various matters specified in the Directive, including the types of activities that may be outsourced and their total extent, processes of due diligence vis-à-vis service providers, matters to be included in the outsourcing contract, the assimilation of an outsourcing risk-management program, and the development of business-continuity plans.

### **Senior management (Sections 13–14)**

13. Senior management is the executive arm of the Board of Directors; it helps the Board to carry out its responsibilities. Consequently, it is in charge of formulating an outsourcing policy and plan and of ensuring their implementation by the banking corporation, *inter alia* by creating an organizational structure, working processes and procedures, and controls to make sure that the outsourcing will be managed in accordance with the policy set forth.
14. Senior management shall periodically review the development of the banking corporation's exposure to outsourcing risks, including identification, assessment, management, and mitigation of said risks in accordance with the policy set forth, and shall report the results of said review to the Board of Directors. Whenever the eventuation of a material outsourcing risk is feared, or when such a risk does eventuate, management is expected to serve the Board of Directors with immediate notice to this effect.
15. The Chief Risk Officer shall ensure the performance of outsourcing accords with the risk-management principles set forth in Proper Conduct of Banking Business Directive 310, "Risk Management," and the provisions of the directive on risk management.

### **Internal audit (Sections 15–16)**

16. Internal audit shall incorporate outsourcing activity into its work program including a review of risk management and material activities outsourced, as set forth in Proper Conduct of Banking Business Directive 307, "Internal Audit Function."
17. In view of the expected increase in the use of outsourcing and the risks pertaining to this manner of activity, particularly in terms of information and cyber security and protection of the privacy of customers' data, the internal audit function should be involved in due-diligence processes at the earliest stages of the outsourcing of

a material activity and should review said due-diligence processes in such a manner and on such a scale as it shall determine.

## **Chapter C—Restrictions on Outsourcing**

### **Operations that may not be outsourced (Section 17)**

18. The Directive specifies several operations that shall not be outsourced:
- (a) Duties of the Board of Directors and senior management, particularly in determining strategies and policies, determining risk appetite, and controlling and supervising risk-management processes. These duties constitute the core activities of the Board and senior management; for this reason, these organs have responsibilities that cannot be transferred to any entity outside the banking corporation.
  - (b) Any decision on opening or closing a customer account; creating (underwriting) a loan, or receiving a deposit. These are core activities of the bank, for which the bank is liable in terms of risk management including compulsory compliance with statutory provisions on prevention of money laundering and terror financing, and in terms of responsibility to customers. This activity, however, is permissible when the service provider invokes the banking corporation's model and does not use its own discretion in deciding on creating a loan or accepting a deposit, and when an account is opened for the sole purpose of managing a loan already created or managing a deposit already received. This activity shall also be permitted where the service provider belongs to the same banking group.

## **Chapter D—Contracting with a Service Provider**

### **Due-diligence check of a service provider (Sections 18–21)**

19. A banking corporation shall perform due diligence vis-à-vis a service provider on the basis of criteria that it shall establish, by which it may evaluate the service provider's ability to carry out the activities that will be outsourced to it effectively, reliably, and on a high standard, as well as the potential risks of contracting with the service provider. A banking corporation is expected to perform said due diligence not only before a service provider is chosen but also periodically and, particularly, before the contract is renewed.
20. When a service provider abroad is used, a banking corporation is expected to examine, before contracting, the provider's political, economic, legal, and regulatory environment in order to minimize the additional risks embedded in an activity abroad. In respect of said environment, the banking corporation shall make sure that the contracting arrangement does not impair its ability to comply with all legal and regulatory provisions that apply to it and that it can impose effective control on the service provider's activity and perform audits or receive audit reports about it from the entities specified in the Directive. A banking corporation shall also make sure that no infringement of the Supervisor of Banks' ability to exercise h/her powers exists, including h/her ability to receive relevant information about the outsourced activity and to examine potential implications of the export of databases to foreign countries for the banking corporation's ability

to comply with laws and directives that apply to it, *inter alia*, due to the access of said countries' supervisory authorities to the databases.

### **Outsourcing contract (Sections 22–23)**

21. A banking corporation's relations with service providers shall be regularized by means of written contracts that shall be in effect for an adequate period of time and that shall meet accepted standards. The section specifies a list of topics that the banking corporation is expected to consider including in the contract, among others, in accordance with their relevance. Notwithstanding the contents of said section, two items were put in place that the banking corporation must include in the contract: enjoining the service provider against charging a fee or any other payment from the customer for activity that it performs under an outsourcing contract, with the exception of such charging as is allowed by law, in order to minimize potential conflicts of interests, and immediate compulsory reporting to the banking corporation of any breach of data of customers or of the banking corporation or any change that has a material effect on the continued delivery of service.

Below are examples of matters that the banking corporation must consider including in the outsourcing contract:

- (a) Its ability to access all outsourced records and information that are relevant to activities and held by the service provider;
- (b) safeguarding its ability to monitor the service provider in respect of outsourced activity and to conduct auditing activity or receive audit reports produced by recognized entities specified in the Directive;
- (c) upholding principals of information security and protection of privacy;
- (d) terms for termination of the contract.

The Directive stresses that the banking corporation must make sure that the non-inclusion of any of the matters spelled out in Section 23 will not expose it to material risks.

## **Chapter E—Management of Outsourcing Risk**

### **Outsourcing management plan (Sections 24–28)**

22. As outsourcing is put to growing use and as it becomes material in certain banking corporations, it is important to formulate a specific plan for the management of this risk and to allocate adequate resources. A banking corporation shall assess the effect of outsourcing risk on its overall risk profile before entering into a material contract with a service provider and shall update the plan periodically. It shall determine ways to minimize the risks, apply monitoring and control relative to every material outsourcing agreements, and put in place guidelines for action if certain events materialized. The corporation shall designate a person to be in charge of each material contract, who will be responsible for the totality of information and risk assessment relating to said contract. The materiality of an outsourcing contract shall be determined, *inter alia*, on the basis of the considerations specified in the Directive.

### **Business-continuity plan (Section 29)**

23. A banking corporation must put together a business-continuity plan in respect of outsourcing, for each material outsourcing arrangement. It shall also make sure that the service provider has its own business-continuity plan in place. The banking corporation shall review its ability, where necessary, to turn to an alternative service provider or to transfer the outsourced activity back in consideration of costs, construction time, and types of activities outsourced.

## **Chapter F—Outsourcing of Special Activities**

### **Contracting with a service provider who works with customers (Section 30)**

24. When it contracts with a service provider who works with customers, a banking corporation must make sure that it continues to honor its obligations to the customers and that its outsourcing cause them no harm. Consequently, the corporation must comply with various guidelines, including placing the service provider under controls and monitoring to make sure that it treats customers fairly and transparently, ensuring that the service provider gives its staff adequate training in how to behave with customers, and making sure that the remuneration mechanisms for the service provider and its staff take fairness toward customers into account. When a service provider refers a customer to the banking corporation for the extension of credit, the banking corporation must take steps to review the customer's total indebtedness and repayment ability and assure the suitability of the credit to the customer's needs. The banking corporation shall also mark loans that are approved pursuant to referral of a service provider and shall subject them to more intensive monitoring.

### **Outsourcing of Internal Auditing Activity (Section 31)**

25. A banking corporation may outsource internal-audit activities subject to the provisions of Proper Conduct of Banking Business Directive 307, "Internal Audit Function," including approval from the Board of Directors for the outsourcing of internal-audit activities, assuring the independence and objectivity of the internal-audit function, and not obtaining outsourced internal-audit services from the external auditor.

### **Outsourcing Associated with Compliance and Prohibition of Money Laundering and Terror Financing (Section 32)**

26. A banking corporation may outsource certain activities of the compliance function and shall make sure that service providers operate in accordance with all relevant laws and directives concerning the prohibition of money laundering and terror financing.

## **Chapter G—Reporting to the Banking Supervision Department**

### **Compulsory reporting to the Supervisor of Banks (Sections 33–34)**

27. Given the expected increase in the use of outsourcing and in its related risks, particularly the handling of sensitive customer information, banking corporations

that wish to outsource material activities must report this to the Supervisor of Banks as soon as possible after the decision is made at the senior-management level and must explain the rationale behind their decision.

The Supervisor may advise the banking corporation, within twenty-one days, of his or her intention of examining the outsourcing activity or not. The results of the Supervisor's continued examination of the activity shall be presented to the banking corporation within ninety days, provided the corporation has given the Supervisor all the material that s/he requested for said review.

28. The banking corporation shall apprise the Supervisor of Banks of any development that has a material effect on the service provider and on the banking corporation's ability to honor its obligations to its customers or to the Supervisor of Banks.

## **Chapter H—Effective Date and Transitional Provisions**

### **Effective date and transitional provisions (Sections 35–39)**

29. The Directive shall go into effect on March 31, 2020, in order to give banking corporations reasonable time to prepare for compliance with the requirements. A banking corporation that completes its preparations for all requirements of the Directive before this date may apply the Directive from the date on which it completes the preparations and, on that date, the provisions spelled out in Section 40 of Directive 359, "Banking Corporations' Ties with Intermediaries," and the relevant sections of Directive 357, "Information Technology Management," will also be nullified.
30. In respect of contracts executed before the promulgation of this Directive, an additional period of three and one-half years is given (bringing the total to five years) in order to align the contracts with the Directive to whatever extent necessary.
31. In regard to using a service provider in order to approach households deliberation for the purpose of referring them to the banking corporation to take credit, it is stated that the beginning of this activity shall be permissible only after the Credit Data System is activated and after the Supervisor amends this section of the Directive. During this time, said referral will be allowed provided one of the conditions set forth in the Directive is satisfied: no remuneration whatsoever is given to the service provider, credit is offered to the customer after the customer's deliberate approach to purchase a product, or when the service provider is a member of the banking group. It is stated for clarity that the term "product" includes a service. This section is irrelevant for credit-card companies that will be allowed to contract with a service provider for said activity from the effective date (as established in the Directive or on the date when said company completes its preparations for the Directive).
32. In addition to the reporting requirements in Section 33, a banking corporation shall report a non-material contract with a service provider for the referral of households for credit for a term of two years from the date on which this Directive is promulgated; afterwards, the Supervisor of Banks shall consider the need for its extension. This reporting is required in order to allow the Department to monitor the activity in question, which is essentially new.

**Treatment of existing directives and authorizations (Sections 40–41)**

33. This section specifies the directives that shall be nullified on the effective date and the requisite treatment of authorizations and permits issued to banking corporations in the past in areas to which the Directive applies, including authorizations in accordance with Section 30(a)(3) of Directive 357.

**Revised file**

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

<b>Insert page</b>	<b>Remove page</b>
(10/18) [1] 359A-1-8	-----

Respectfully,

Dr. Hedva Ber

Supervisor of Banks