Business Continuity Management

Introduction

1. The centrality of the banking system in financial intermediation, the advancement of economic activity, and processes of settlement, as well as the importance of the public's confidence in the ability of the banking system to function continually, make it essential to assure the system's resilience to major operational disruptions. To attain this goal, each banking corporation must assimilate a comprehensive framework for business continuity management in a manner suited to the characteristics of its activity, its exposure to risks, and its business strategy.

   A comprehensive framework for business continuity management will enhance the banking corporation's resilience when external or internal events cause significant operational disruptions and will mitigate the possible adverse impact of such disruptions on business activity continuity, proper operation of payment and settlement systems, provision of banking services to the public, reputation, profitability, depositors, and holders of the banking corporation's securities.

Application

2. This Directive shall apply to all banking corporations as defined in this Directive.

Definitions

3.

"Banking Corporation"	As defined in the Banking (Licensing) Law, 5741-1981, including an auxiliary corporation that is a credit-card company and/or an auxiliary corporation that is defined as a critical enterprise.
"Critical enterprise"	As defined in the Emergency Labor Service Law, 5727-1967.
"Emergency"	A period of time in which a state of emergency system is activated per Government Resolution 1716 of Sivan 29, 5746 (July 6, 1986), Government

	Resolution 1080 of Adar A 7, 5760 (February 13, 2000), and any other government resolution relating to this matter, the declaration of a special situation in the home front under Section 9c of the Civil Defense Law, 5711-1951, or a declaration of a state of emergency by the Supervisor.
"Business continuity"	A situation in which the business operates in a continual and disruption-free manner.
"Business continuity management"	A whole-of-business approach that includes policies, standards, and procedures for ensuring that certain operations may be performed or resumed in a timely fashion in the event of disruptions.
"Business continuity plan"	A comprehensive written plan of action that sets out the procedures and systems necessary to maintain business continuity or to restore the operation of the banking corporation in the event of disruptions.
"Resilience"	The ability of a banking corporation to absorb the impact of a major operational disruption and continue to maintain critical operations or services.
"Critical operation or service"	Any activity, function, process, or service, that are crucial to maintaining the banking corporation's stability and the public's confidence, to protecting its customers and depositors, and to the continuous operation of payment systems to the extent that depends on the banking corporation. Determining whether a certain operation or service is "critical" depends on the nature of the relevant banking

corporation. In particular, processes that are required for continual operation of critical sites and payment and settlement systems will be considered as critical operations or services.

"Major operational disruption" A disruption that has a grave effect on ordinary business activity and that causes economic damage to a large area and to the public that inhabits it, such as a situation that prompts a declaration of emergency. A major operational disruption typically affects physical infrastructure and may be caused by a broad range of events such as war, terror attacks, earthquakes, weather-related events, strike, or other malicious acts or occurrences that cause widespread damage to physical infrastructure.

Other events, such as technological viruses, pandemics and other biological incidents, will not necessarily cause widespread damage to physical infrastructure but nonetheless may cause major operational disruptions via their effect on the ordinary activity of physical infrastructure in other ways.

Events that have the greatest impact are called "extreme events." They typically involve one or more of the following scenarios: destruction of, or severe damage to, physical infrastructure and facilities, loss or inaccessibility of personnel, or restricted access to the affected area.

"Reference scenario"	A possible outline of security, operational, intra-corporate, economic or other incidents in respect of which a major operational disruption is expected to the banking corporation and which is considered a relevant outline for planning a response.
"Main site"	A site that provides a critical operation or service to all customers of the banking corporation, excluding a branch.
"Alternate site"	A site held in a state of readiness and meant for use in an event that necessitates the maintenance of the banking corporation's business continuity. This term applies equally to the working space and to technological needs.
"Critical site"	Main site and alternate site.
"Disaster recovery site"	An alternate site used to recover data and information systems in emergency events.
"Recovery"	The rebuilding of specific business operations following a disruption to a level sufficient to meet outstanding business obligations.
"Recovery objective"	A pre-defined goal for recovering specific business operations and supporting systems to a specified level of service (recovery level) within a defined time after the occurrence of the disruptions (recovery time).
"Recovery level"	An element of a recovery objective. The recovery level is the target level of service that will be provided in respect of a specific business operation after a disruption.

"Recovery time"	An element of a recovery objective. Recovery time is the duration of time to recover a specific business operation. The recovery time has two components: the duration of time from the disruption to the activation of the business continuity plan and the duration of time from the activation of the business continuity plan to the recovery of a specific business operation.
"Communication protocols"	Established procedures for communicating that are agreed in advance by two or more parties within the banking corporation or between a banking corporation and parties external to it that describe, *inter alia*, the nature of the information that should be shared with various internal and external players and the method to be used in treating certain types of information (e.g., public and non-public information).
"Core branch"	A branch that has a protected space approved by the IDF Home Front Command, prepared in advance, for an emergency, which is designated in advance to be opened in a state of emergency.
"Mobile branch"	A branch that may be moved about and operated in different locations, including from a suitable motor vehicle.
"Governor's permit"	A general permit allowing banks to open and relocate branches in an emergency, dated July 11, 2010.

Responsibilities of the board of directors and senior management

4. The banking corporation's board of directors and senior management shall relate to business continuity risks and their control as part of the overall framework for risk management, as follows:
   (a) The board of directors shall ensure that senior management has a comprehensive business continuity management framework, and shall oversee it appropriately on an ongoing basis.
   (b) The board of directors shall approve senior management's risk management and control policy in the area of business continuity.
   (c) Senior management shall appoint a business continuity manager and define his/her responsibilities and authorities.
   (d) Senior management shall appoint a crisis management team composed, *inter alia,* of members of senior management. The team shall include main decision-makers and professionals from the range of departments at the bank, in order to assure optimum crisis management and decision-making ability during stress situations.
   (e) Senior management, per approval of the board of directors, shall assign adequate resources for the application and assimilation of the business continuity plan in relation all of the banking corporation's activities.
   (f) Senior management shall discuss the refreshing and updating of the business continuity plan once a year, or whenever a material change occurs in the activity and risk environment, so that the plan will reflect the changing characteristics of the banking corporation's activity, complexity, and size.
   (g) The board of directors and senior management shall establish a periodic reporting format that will allow each of them to discuss the effectiveness of the business continuity management framework.

Part A—Business continuity management

Formulation of a business continuity management framework

5. The business continuity management framework shall be formulated on a firm-wide basis and shall be integrated into the banking corporation's risk management program. The business continuity management framework shall refer mainly to the possibility of a major operational disruption at the banking corporation, but is to take into account the possibility of such a disruption in the overall banking system. Implementation in an emergency is detailed below in Part B, under "Critical Service Level Objectives". The framework, as noted, is to include at least the following four elements:

   (a) **Business Impact Analysis**—a dynamic process for identifying critical operations and services, including those that are mutually dependent, key internal and external dependencies and appropriate resilience levels. The analysis is to examine the risks and the potential impact of various disruption scenarios on a banking corporation's operations and reputation.

   The banking corporation shall test national and other scenarios that may affect critical processes and services in the short, medium, and long terms, and shall update them in accordance with developments.

   (b) **Recovery strategy**—sets recovery objectives and priorities that are based on the implications of the business impact analysis. The objectives relate, *inter alia,* to the level of service that the organization shall aim to provide in the event of disruptions and the framework for the final restoration of business operations.[1]

[1] The ultimate goal of the business continuity program is full operational recovery to the point at which the banking corporation can resume ordinary business activity. Most programs establish a continuum in the operational recovery process in accordance with the effect of each operation on business, focusing first on the banking corporation's most critical operations.

Recovery objectives must reflect the risk that each banking corporation represents to the operation of the financial system, and define recovery levels and recovery times expected for critical processes or services.

(c) **Business continuity plan**—sets detailed guidance for implementing the recovery strategy. The business continuity plan specifies duties and responsibilities for managing operational disruptions and provides clear guidance regarding the delegation of powers in the event of disruptions that disable key personnel. The plan also clearly establishes decision-making powers and defines triggers for its implementation.

The business continuity plan shall include all critical processes and services, resources and infrastructures at the relevant units and activities of the banking corporation and its overseas branches.

(d) **Risk monitoring and testing program**—A banking corporation shall assimilate its business continuity plan among its staff and shall monitor and validate it regularly, *inter alia* by establishing testing and training programs. The program shall specify the matters being tested and its objectives, its frequency, the methodology chosen, and the existence of an independent control body that will inspect the test as it is being performed, the method of reporting the results of the test, a process for identifying gaps in the existing business continuity plan, and updating the plan accordingly.

Business continuity plan

6. (a) A banking corporation shall have a business continuity plan in place that will assure its ability to operate continually, limit its losses in the event of a serious disruption of its business, and allow its operation to recover in the event of a disaster. A banking corporation is required to examine which reference scenarios are liable to impact on critical operations and services in the short, medium, and long term, and to update them in accordance with developments.

(b) The business continuity plan shall provide action guidelines for an immediate response to a major operational disruption. The plan shall relate to all critical

processes and services but shall also take into account requisite long-term measures for full recovery of activity to routine condition.

(c) In formulating its business continuity plan, the banking corporation shall relate to the following elements at least:

(1) **Human resources—**Human resources are a critical element in the fulfillment of the business continuity plan. On the basis of the business impact analysis, responsibilities and powers shall be assigned to members of management, work teams, internal and external service providers, and others. Also, a backup plan for personnel who are essential to the operation of critical operations and services, including in a case of a strike, shall be formulated, and a professional crisis management team shall be specified.

(2) **Communications and media relations**—clear and systematic communication during a major operational disruption is essential in managing the crisis and in maintaining public trust. The business continuity plan shall include communication protocols for managing all communication interfaces relevant to the banking corporation in a major operational disruption, including in a state of emergency: employees, emergency personnel, regulators, external suppliers, customers, media, correspondent banks, etc. The plan shall include updated and accessible lists of contacts and various communication methods for the dissemination of information to customers, service providers, and regulators, so that they will know how to contact the institution even if ordinary communication channels are disabled. In addition, the banking corporation shall formulate an official media relations plan and integrate it into its business continuity plan.

(3) **Technological issues**—The business continuity plan shall address all technological elements that are necessary to maintain business continuity and/or recovery of operations.

(4) **Relocation of critical operation or service**—The business continuity plan shall give expression to the transfer of critical operations or services to a new location.

(5) **Payment and settlement systems**—The business continuity plan shall include alternate arrangements for continued operation in the event of operational disruptions, from the following perspectives: (a) Cash withdrawal (including from ATMs), (b) providing service to make payments through the various e-banking channels and through branches, (c) operation of the Zahav (RTGS) and Paper-based (Checks) Clearing House systems, with an emphasis on activity vis-à-vis CLS. These alternate arrangements may include setting withdrawal limits for customers without approval, backup agreements with third parties, specifying manual working processes, and, of course, the creation of backup systems for immediate activation at an alternate site.

(6) **Cash and liquidity needs—**major operational disruptions may, on the one hand, intensify the public's demand for cash and, on the other hand, trigger a financial crunch with implications for liquidity. The business continuity plan should address all aspects of cash and liquidity, including having an adequate and efficient emergency funding plan in place that clearly determines strategies for the treatment of liquidity difficulties.

(7) **Manual work alternatives—**The business continuity plan shall include, as the case may be, procedures for manual working processes, approved in advance by the management of the banking corporation, as an alternative to critical operations and services. In this regard, the banking corporation shall maintain backup records on customer accounts (account numbers, addresses, state of account, account balance, etc.).

(8) **Reinforcement of control systems**—When operational disruptions occur, risk levels rise due to potential changes in the working environment, personnel, equipment, etc. In any analysis of business implications, the

risks should be reassessed, and a strategy for their prevention and minimization should be formulated and integrated into the business continuity plan.

(9) **Business planning and project management—**To maintain and update the business continuity plan, a banking corporation shall make business continuity considerations part of every relevant business decision, including decisions relating to the planning and management of new projects.

(10) **Change control policy—**Such a policy should reflect the fact that when changes are introduced in operational systems, applications, or infrastructures in the production environment that support critical processes and services, all copies of the backups of these systems should also be updated. In addition, whenever a new or improved system that requires new hardware, additional capacity, or other technological changes is implemented, a banking corporation should make sure to update its business continuity plan to the extent necessary and to make its recovery site capable of supporting the new production environment. The change control policy should also make it possible to implement changes rapidly in the event of an operational disruption.

(11) **Backup of data—**A banking corporation shall have data synchronization procedures in place that will permit the accurate and up-to-date retention of data at the disaster recovery site. A banking corporation shall have procedures in place for information retrieval, within a reasonable period of time, in a situation of a failure event at the main site before the data of the business day have been backed up. The banking corporation must back up its data in a manner that will assure recovery even in cases where its main site and its disaster recovery site are damaged concurrently.

(12) **Crisis management—**A banking corporation shall designate, in its procedures, a senior authority who may declare a crisis event and the

responsibilities of a crisis management team for the internal application of the business continuity plan and the assurance of the banking corporation's conduct vis-à-vis outside players such as regulators, government offices, and emergency organizations.

(13) **Information security incidents**—Banks shall develop a policy of response to information security incidents and shall adequately integrated it into their business recovery plan. An information security incident occurs when an unauthorized player attempts, successfully or not, to invade, use, sabotage, or destroy information systems or customer data. In the event of an unauthorized intrusion, the banking corporation's computer systems may crash and confidential information may fall into incorrect hands. An important element in the response to information security incidents is the division of responsibilities for evaluation of, response to, and management of IT indicents and the development of guidelines for staff in regard to escalation and reporting procedures. Senior management shall determine who shall be responsible for declaring an incident and for reconstructing the affected computer systems from the moment the incident ends. The holder of this responsibility must have the expertise that is needed for a rapid and appropriate response.

(14) **Remote access policy**—Working procedures for remote access shall be part of the business continuity plan. Since bank facilities will be inaccessible in certain emergenies, it may be necessaty to give remote access to staff or outside serivce providers. The remote access policy shall be approved by senior management and shall address itself to the risks associated with the policy and the maintenance of appropriate control and information security mechanisms.

(d) The business recovery plan shall be assimilated among critical staff and drilled at all banking corporation units in accordance with a program that the bank shall establish. The assimilation plan shall help, *inter alia,* to test the bank's

ability to operate critical operations and services in the event of a shortage of key personnel.

(e) To assure the successful application of business continuity plan, a banking corporation shall establish solid ongoing working relations with community officials (e.g., local authorities) and government institutions, including national infrastructure officials, for optimum coordination of expectations and evaluation of risks. Integrating these expectations into the business continuity plan and conducting joint drills will enhance the effectiveness of the business continuity plan.

Insurance

7. While adequate insurance coverage is no substitute for an effective business continuity plan, it may help to reduce losses and damage occasioned by major operational disruptions, and thus it is important. Insurance coverage shall be chosen on the basis of a business impact analysis and a risk assessment. At least once a year, the banking corporation shall examine the adequacy of its insurance coverage with regard to its most recent risk profile.

Business continuity of critical process vendors and service providers

8. (a) A banking corporation shall act to mitigate the risks that flow from dependency on vendors and service providers for its critical processes.

(b) A banking corporation shall ensure that its contract with a vendor/service provider obliges the vendor/service provider to serve the banking corporation even in an emergency, in accordance with the service level agreement specified in the contract.

(c) The banking corporation shall assess the vendor's/service provider's ability to maintain business continuity so that the banking corporation will continue to recent the relevant service under various scenarios.

(d) In accordance with the assessment set forth in Subsection (c) above, the banking corporation's contract with the vendor/service provider shall include reference to matters such as:

(1) the vendor's/service provider's responsibility for having a business continuity plan in place;

(2) the banking corporation's right to receive the vendor's/service provider's business continuity plan;

(3) the banking corporation's right to participate in the vendor's/service provider's drills and/or to obtain the findings of the drill;

(4) the banking corporation's right to conduct a periodic review of the vendor's/service provider's business continuity plan or to receive a report from some other reviewer who is acceptable to the banking corporation.

(e) Notwithstanding the foregoing, Sections (b) and (d) need not be included in a contract with suppliers of national infrastructures.

Alternate site

9. (a) A banking corporation shall locate its alternate sites so as to mitigate the probability of a similar effect of any particular emergency scenario on the alternate sites and the main site, including an effect on elements of physical infrastructure (electricity, communication, etc.) that the sites use.

To mitigate the probability that both sites will be impaired by the same scenario, including the possible blockage of access routes, the banking corporation shall ensure, at the very least, that the alternate site will be located outside the municipal boundaries of its main site.

(b) A banking corporation shall leave enough equipment and information at the alternate site to ensure the continuity of its business activity if its main site is severely damaged.

(c) In determining the alternate site, the banking corporation shall relate to the following parameters *inter alia*: size of the site, the capacity of work there, and the services that must be delivered in accordance with the specified levels of

service, with reference to the duration of the operational disruption (short, medium, and long term). In cases where the alternate site is located at a facility that is used for regular daily activity, the banking corporation shall ensure that the is capable of accommodating additional business functions when the main business location becomes unusable.

(d) The alternate site shall be immediately available (24/7) for work, and personnel slots shall be the established for it.

(e) The banking corporation shall make all efforts to avoid having the alternate site operated by a third party. Nevertheless, if the operator of the alternate site is a third party, the banking corporation shall ensure that said third party is able in all ways to keep the site maintained and ready for an emergency (by auditing the third party, executing a contract with it, etc.).

(f) A banking corporation shall not share an alternate site with another banking corporation that is outside the banking group if there is concern that this will negatively impact the implementation of its business continuity plan.

(g) A banking corporation shall take into account of the inherent system risk that exists if its critical sites are geographically concentrated with those of other banking corporations.

(h) A banking corporation that is a joint service company that is a key player in the functioning of the financial system shall have duplicate information systems of high availability, such as Active-Active, in place for its critical services, between its main site and its alternate site.

Protection of critical sites

10. (a) A banking corporation shall act to protect its critical sites with the intention of maintaining continuity and constancy in the provision of critical services, all in accordance with accepted professional standards.

(b) The following are the guiding principles for minimum protection of the various critical sites:

(1) A main or alternate site, at least one of the two, must be protected against conventional warfare.

(2) A main or alternate site, at least one of the two, shall be earthquake resilient.

In a case where a main critical site is not able to withstand an earthquake, the banking corporation shall maintain an operative plan for making critical

services available at the alternate site, in accordance with the service targets set out in Section 12.

(3) Beyond what is stated in this Section:

(i) Every critical site that serves for data processing shall be protected against conventional warfare.

(ii) For a joint services company that serves as a key element in the functioning of the financial system, every critical site shall be protected against conventional warfare and shall be able to withstand an earthquake.

(4) When constructing a new critical site, the appropriate protection for all reference scenarios, national and otherwise, must be ascertained. In particular, the Tier level shall not be less than 3 for computer sites.

(5) A subsidiary company of a banking corporation may rely on the parent company's critical site for the purpsoe of making critical services available when a reference scenario is realized, and in accordance with the service targets set out in Section 12. The parties must arrange this in an appropriate agreement, and must periodically assess the possibility of realization.

(c) In extenuating cases, a banking corporation that believes that some of the principles for minimum protection of the critical sites are not applicable to it,

may appeal to the Supervisor of Banks to coordindate their applicability or manner of implementation regarding it.

10a. A banking corporation shall consistently act to protect its branches in accordance with Home Front Command guidelines.

Internal audit

11. (a) The comprehensive business continuity management framework shall be subject to periodic auditing by the internal audit function.

(b) Internal audit shall review the testing program periodically to evaluate its effectiveness.

(c) The findings of the testing of the business continuity plan shall be reported to internal audit on a regular basis.

Part B—Levels of critical service objectives

12. As a rule, the banking system shall aim to maintain business continuity to the greatest extent possible. However, during emergencies or a situation of major operational disruptions, it is possible that major operational disruptions (system-wide or bank-specific) may adversely impact the ability to provide full service. Therefore, a banking corporation shall prepare for the continuation of its business activities in a manner that will ensure the ongoing attainment of the following service level objectives at least:

(a) Within several hours of the beginning of disruptions

(1) Will make an effort to ensure uninterrupted operation of its payment systems, including its interfaces with the Zahav (RTGS) system.

(1a) Will make an effort to ensure uninterrupted operation of cash withdrawal from ATMs, as follows:

i. Banking corporations that operate ATM cash withdrawal services shall be prepared, at any time and in all localities, to refill the machines during an emergency before they run out of cash.

ii. Switch and communication services shall operate in a way that will allow the public to withdraw cash from all banks' ATMs.

(2) It shall be possible to use credit cards to make purchases at places of business.

(3) In an emergency, the banks' branches shall operate as set forth in Section 13 of the Directive.

(4) If the banking corporations sign an arrangement allowing cash withdrawals via checks by customers of other banking corporations, the banking corporations in the arrangemetns shall be prepared to implement it in accordance with guidance from the Supervisor.

(5) A banking corporation shall provide the public with critical information, through the operation of an appropriate information call center (such as a hotline), the phone number of which shall be publicized.

(6) Banking corporations shall prepare for the continued provision of banking services (information and transactions) to their customers through direct channels such as on-line banking and telephone call center.

(7) Banking corporations shall prepare to resume settlement activity vis-à-vis all relevant clearing houses in accordance with rules set forth for each respective system. Banking corporations that operate settlement facilities shall take measures to reactivate them.

(b) Within a maximum of 24 hours from the beginning of disruptions

(1) Banking corporations shall be ready to activate emergency mobile branches in places where the "regular" bank branches cannot provide services, as set forth in Section 14 of the Directive.

(2) Transfers of funds from and to locations abroad.

(3) Resumption of activity vis-à-vis capital-market institutions (provident funds, advanced training funds, etc.) and vis-à-vis locations abroad.

(c) Levels-of-service objectives to be attained within several days, at the most, of the beginning of disruptions

(1) Emptying of service boxes at branches that are not active in emergencies.

(2) Banking corporations shall be ready to activate a program of dispensations for population groups that stand to be harmed by the emergency, e.g., mobilized soldiers, members of their families, and business owners. Some of the arrangements shall be the results of the banking corporation's policy and others shall be made by approval of the Supervisor as set forth in Section 15 of the Directive.

Opening of branches in an emergency

13. (a) The policy on opening branches during an emergency shall be to strive to open all branches per guidance from the Supervisor of Banks and subject to instructions from the security forces, including the IDF Home Front Command.

(b) Banking corporations shall designate a minimum of 25 percent of the total number of their branches as "core" branches and shall ensure the appropriate geographic dispersion of "core" branches.

(c) Banking corporations shall strive for the activation of all branches that are defined as "core" branches as soon as the state of emergency begins. The activation of a branch means at least the provision of services via the branch's self-service machines or the opening of the branch to the public. A banking corporation shall continue to provide banking services through alternative means, to the extent possible given the circumstances, even if some branches do not open due to the emergency situation.

(d) Banking services provided in branches activated during an emergency shall include, at least, providing customers with information on the state of their accounts and carrying out basic banking services, such as: withdrawing and depositing cash, withdrawing and depositing checks, and interbank and intrabank transfers.

Relocation of branches in an emergency

14. (a) Once the Supervisor of Banks has declared a state of emergency for the purpose of implementing the Governor's permit (set below in Appendix A), in full or in part, a banking corporation may:
    (1) temporarily relocate a branch, including to a location that another bank allows it to occupy, provided that its staff continue to run the relocated branch;
    (2) conduct business at mobile branches as set forth in Section 14 of the Directive;
    (3) provide basic banking services to its customers by means of branches of other banks or of the Postal Bank, subject to arrangements that the Supervisor shall approve in advance.

    (b) A banking corporation shall serve the Supervisor with written notice about the temporary relocation of a branch or the activation of a mobile branch.

Mobile branches

15. (a) Each banking group or independent bank that operates a network of branches comprised of at least 30 branches shall be prepared to activate mobile branches in a state of emergency, in accordance with the circumstances that evolve.

    (b) The minimum ratio of mobile branches shall be one for every 50 branches in the possession of the banking corporation on a group basis, in round figures.

    (c) A banking corporation shall determine in its policy how many of its mobile branches will be of the kind that operate out of a suitable motor vehicle.

    (d) In accordance with the authority of the Supervisor of Banks under Section 2.5 of the Governor's permit, a banking corporation shall deploy to offer the following banking services at a mobile branch:
        (1) withdrawal of cash, including by customers of other banks;
        (2) deposit of cash;
        (3) drafting and depositing of checks;
        (4) operating service boxes;

(5) transfers from account to account.

(e) A banking corporation that wishes to offer additional banking services shall do so only after obtaining prior approval from the Supervisor of Banks.

(f) Banking corporations shall ensure the availability of the relevant infrastructures for the operation of the mobile branch.

(g) Banking corporations shall assess the risks associated with the activation of mobile branches and shall have an appropriate working procedure and adequate means of control and information security in place.

Dispensations for the population

16. (a) Within the framework of the emergency deployment, temporary dispensations from Proper Conduct of Banking Business Directives are necessary so that the population can more easily obtain banking services in emergencies.

(b) The dispensations specified in Appendix B shall go into effect only when the Supervisor of Banks so declares. The timing and duration of the dispensations may vary from place to place, as may the geographical area to which the dispensation applies. These parameters shall be expressed at the time the Supervisor of Banks announces that the dispensation will go into effect.

Identifying persons who lack official documentation

17. (a) Banking corporations shall develop tools for the identification of customers who lack official documentation, maintaining adequate controls and limiting exposure to risk.

(b) An internal working procedure for the identification of customers who lack official documentation in a state of emergency shall go into effect after the bank obtains approval from the Supervisor of Banks.

Appendix A

Bank of Israel

The Governor

General Permit to Banks for the Opening and Relocation of Branches in a State of Eemergency

Under the Banking (Licensing) Law, 5741-1981

By virtue of the authority vested in me by Section 28 of the Banking (Licensing) Law, 5741-1981, and after consulting with the Licenses Committee, I hereby authorize a bank, subject to the declaration by the Supervisor of a State of Emergency for the purposes of this Permit:

1. to temporarily relocate a branch, for a period of time that shall end, at the latest, upon the cancellation of the Supervisor's declaration as aforesaid, to a new location in Israel, provided that the Supervisor be served with notice near to the time the relocation takes place;
2. to conduct business in Israel with its customers and to provide services to customers of other banks that it controls (hereinafter: **controlled banks**) at mobile branches, under the following conditions:
   2.1 In this Permit, a "mobile branch" is a branch that is movable and that may be operated in different locations, including from a suitable motor vehicle;
   2.2 The mobile branch shall carry appropriate signage of the bank;
   2.3 Activity vis-à-vis customers shall take place only on the premises of the mobile branch. Transactions with customers shall be documented in the records of the bank or of the controlled bank;
   2.4 Employees of the mobile branch shall be employees of the bank and/or of controlled banks and shall be adequately trained for the discharge of their duties;

2.5 The Supervisor shall determine the minimum banking services that the bank shall provide at the mobile branches and shall approve the range of possible banking services at the mobile branches;

2.6 The controlled bank shall be fully responsible vis-à-vis its customers for any transaction as aforesaid. The bank and the controlled bank shall set conditions for the imposition of the bank's responsibility on the controlled bank;

2.7 The Supervisor shall be served with notice, near to the time of the opening and closing of the mobile branch, including the number of open mobile branches of the bank on a given day and such additional details as the Supervisor shall request;

3. to provide its customers with basic banking services via permanent or mobile branches of another bank, or via the Postal Bank, under an arrangement comprised of terms that the Supervisor of Banks shall approve.

The Supervisor is entitled to declare a state of emergency for the purpose of this Permit, in whole or in part.

[Signed]
Stanley Fischer
Jerusalem, Tammuz 29, 5770, July 11, 2010

r1003804

Appendix B

Possible Dispensations for the Population in a State of Emergency

Below is a breakdown of possible dispensations for the population that shall go into effect when the Supervisor declares a State of Emergency for the purpose of implementing the dispensations. It is suggested that the dispensations be read together with the original text of the Directives.

1. **Proper Conduct of Banking Business Directive 325: Management of Credit Facilities in Current Accounts**
   a. Notwithstanding the provisions of Section 8 of the Directive for the purpose of limitation of sums, when the Supervisor declares a State of Emergency and, at the most, up to 30 days after the cancellation of the declaration, a banking corporation may refrain from applying the provision of the Directive to overdrafts in sums that shall not exceed the sum set by the Supervisor in his/her announcement.

2. **E-banking Directives:**
   a. An easing in remotely signing up for e-banking services, and an easing in means of personal identification and verification required for carrying out e-banking activities during the period declared a State of Emergency by the Supervisor of Banks. Said easing is for the period declared by the Supervisor to be a State of Emergency, and when that period ends, the processes are to be completed vis-à-vis the customers who signed up for e-banking services during that period.
   b. A banking corporation shall assess in advance the risks related to operating the lenient process and accordingly establish compenating controls, such as limiting sums and sending an SMS after a transaction is carried out.

c. Notwithstanding the provisions of Section 7 of Proper Conduct of Banking Business Directive 420 during the period declared a State of Emergency by the Supervisor of Banks, a banking corporation may refrain from sending notices by post to customers who requested to receive notices via communcation channels, provided provided that said notices are sent out as the Directive and the due diligence rules require once the State of Emergency has ended. To remove any doubt, this easing does not apply to the obligation to send a notice via personal delivery pursuant to the Banking (Service to Customer) Law (Sections 5a1 and 17a).

d. Notwithstanding the provisions of Section 8(b) of Proper Conduct of Banking Business Directive 439, during the term of the Supervisor's declaration of a State of Emergency, a banking corporation may carry out the cancellation of a standing debit authorization by telephone instruction as well.

3. Proper Conduct of Banking Business Directive 358: Transaction of Business outside the Banking Corporation Offices

a. Notwithstanding the provisions of Section 3 of the Directive, during the term of the Supervisor's declaration of the State of Emergency, for the purpose of applying the Governor's general permit to banks to open and relocate branches in a State of Emergency, a banking corporation may invoke the dispensations set forth in the Supervisor's declaration.

***

Updates

Circular 06 no.	Version	Details	Date
2318		Original Directive	Dec. 25, 2011
2422	2	Revision	May 26, 2014
2532	3	Revision	April 9, 2017
2669	4	Revision	September 30,2021