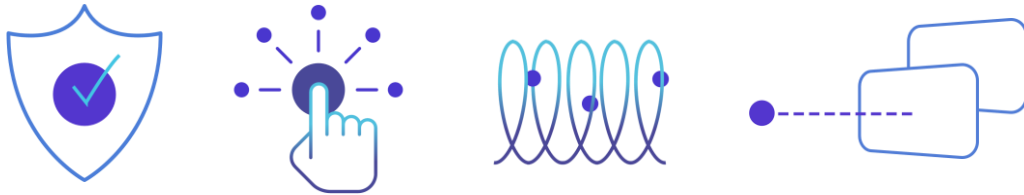


---

# Charge-Card Payment System Rules

---



## Contents

1.	Introduction, Definitions and General Provisions .....	2
2.	System Access and Participation Types .....	<b>Error! Bookmark not defined.</b>
3.	The System's Services .....	<b>Error! Bookmark not defined.</b>
4.	Connection and Management of Terminals .....	43
5.	Approvals Interface .....	<b>Error! Bookmark not defined.</b>
6.	Transaction Collection and Processing Interface .....	<b>Error! Bookmark not defined.</b>
7.	Accounting Interface .....	52
8.	Clearing Interface – Clearing the System's Activity on the RTGS System .....	<b>Error! Bookmark not defined.</b>
9.	Summary Description of the System's Interfaces .....	61
10.	Failure Arrangement in the Payment System .....	62
11.	Cancellation of Participation or Participant Suspension .....	71
12.	SLA .....	75
13.	Information Security .....	80
14.	Risk Management .....	85
15.	Business Continuity .....	85
16.	Dispute Resolution .....	88
17.	Property Rights and Restriction of Use .....	88
18.	<i>Force Majeure</i> and Limitation of Liability and Indemnity .....	89
19.	System Users and Other Engagement Configurations .....	91
20.	Costs/Administration/Miscellaneous .....	94

## 1. Introduction, Definitions and General Provisions

### 1.1. Introduction

Automatic Bank Services Ltd. (the “**Company**” or “**Shva**”) was established and incorporated in Israel in 1978 as a private company pursuant to the Companies Law, 5759-1999. At the beginning of June 2019, after completion of an IPO, the Company became a public company pursuant to the Companies Law, 5759-1999, whose shares are traded on the Tel Aviv Stock Exchange, a reporting corporation, as defined in the Securities Law, 5728-1968. The Company is also a critical state infrastructure pursuant to the Regulation of Security in Public Entities Law, 5758-1998.

Pursuant to the Payment Systems Law, 5768-2008 (the “**Payment Systems Law**”), on 18 July 2013, the “charge-card services” Payment System was declared an audited system, operated by the Company, and therefore the Company is required, pursuant to Section 8 of the Payment Systems Law, to formulate the System Rules as specified herein, as shall be updated from time to time. The System is supervised by the Oversight of Payment and Clearing Systems Department at the Bank of Israel.

### 1.2. Definitions

<b>Irregular Event</b>	An event which deviates from the regular and current activity of the Payment System and/or may affect the regular and current activity of the Payment System.
<b>Payment Method / Credit Card / Charge Card</b>	As defined in Section 11B of the Banking Law (as defined below), and as amended in the Payment Services Law (as defined below). Any reference in these Rules to “card” and/or “cards” is a reference to Payment Method.
<b>Business / Supplier / Trader / Retailer</b>	An entity that operates a Terminal (as defined below), for which purpose it has engaged in a Clearing agreement with at least one Acquirer.
<b>Statutory Requirements</b>	Laws, regulations, orders, as amended or legislated, and requirements, directives and instructions from competent authorities pursuant to any law, as being from time to time, including regulatory requirements, directives and instructions (regulation).
<b>Banking Directives</b>	Banking Directives (Customer Service) (Date of Check Crediting and Debiting), 5752-1992.
<b>Supervision Directives</b>	Directives of the Oversight of Payment Systems, Principles for Financial Market Infrastructures (PFMI), as updated and released from time to time, by the Oversight of Payment Systems at the Bank of Israel.
<b>Payment Instruction</b>	A message which is an instruction to transfer funds.
<b>System / Payment System / Charge-Card Payment System</b>	A “charge-card payments” system operated by the Company, which includes a transaction collection and approvals interface and the

RTGS accounting and Clearing interface, and constitutes an audited system, as defined in the Payment Systems Law.

Any mention of the term “system” refers to the foregoing “charge-card services system”, unless stated otherwise in these Rules.

**Agreements with Participants**

The agreements that were previously signed and/or shall be signed between the Company and the System Participants (jointly and/or severally) in connection with use of the System and/or System subscription agreements and the annexes to these Rules.

**NGO and/or Protocol NGO**

“The Association for Management of EMV Terminals Protocol in Israel” which was established according to a resolution of the Antitrust Commissioner (his then title)<sup>1</sup> to engage in EMV protocol activity, including in the specification and maintenance of the protocol.

**Participant Suspension**

Disconnection of a System Participant with a direct technical connection to the system from the Credit Card Payment System and discontinuation of all activity therewith as specified in the Rules.

**Participants Committee**

A committee established according to the directive of the Oversight of Payment Systems, headed by the System Operator, for purposes of consulting, collaboration and the exchange of information between the System Participants for purposes of formulating the System Rules; informing the Participants (and the Oversight of Payment Systems) of changes to the System Rules and the System’s procedures; discussions on issues and topics relating to activity of the System Participants.

**Banking Law**

The Banking Law (Licensing), 5741-1981, including any and all amendments thereto as being from time to time, including regulations that have been and/or shall be promulgated thereunder from time to time.

**Insolvency Law**

The Insolvency and Economic Rehabilitation Law, 5778-2018, including any and all amendments thereto as being from time to time, including regulations that have been and/or shall be promulgated thereunder from time to time.

**Payment Systems Law**

The Payment Systems Law, 5768-2008, including any and all amendments thereto as being from time to time, including regulations that have been and/or shall be promulgated thereunder from time to time.

---

<sup>1</sup> Resolution regarding conditional exemption from approval of a restrictive trade practice between the banks, both among themselves and with Automatic Bank Services, of 24 September 2017.

<b>Payment Services Law</b>	The Payment Services Law, 5779-2019, any and all amendments thereto as being from time to time, including regulations that have been and/or shall be promulgated thereunder from time to time.
<b>Regulation of the Practice of Payment Services Law</b>	The Regulation of the Practice of Payment and Payment Initiation Services Law, 5783-2023, any and all amendments thereto as being from time to time, including regulations that have been and/or shall be promulgated thereunder from time to time.
<b>System Access Windows</b>	Dates determined by the System Operator (as defined below) on which a new Participant with Direct Technical Connection may begin its activity in the System.
<b>Clearing Account at the Central Bank</b>	A collateral account of the System Participants at the Bank of Israel in the Company's name that was opened for the deposit of the Collateral Funds of the System Participants and is held and managed in escrow by the System Operator for the System Participants for performance of the failure arrangement, including in any case of a failure event of a Participant. The funds held in the said account are not part of the System Operator's assets.
<b>Clearing Account</b>	An account managed on the RTGS System for and in the name of a Participant with direct connection to the RTGS Clearing System, including for purposes of Clearing instructions of other direct and represented participants in a payment system and which is a Participant in the Charge-Card Payment System.
<b>Business Day</b>	Any day, except Bank Holidays (as defined below), Yom Kippur eve, Purim, Tisha Be'Av, and except any day determined by the Supervisor of Banks as a non-Banking Business Day.
<b>Banking Business Day</b>	As defined in the Banking Directives and as specified in PCBB 402 of the Bank of Israel ( <i>Business Day at Banking Corporations</i> ).
<b>Short Business Day</b>	Fridays, holiday eves and mid-holidays (chol hamoed) which are Business Days, except Bank Holidays (as defined below) and any other day determined by the Supervisor of Banks as a non-Banking Business Day.
<b>Regular Business Day</b>	Any weekday, except: Fridays, holiday eves which are Business Days, mid-holidays (chol hamoed), Bank Holidays (as defined below), and any other day determined by the Supervisor of Banks as a non-Banking Business Day
<b>Bank Holidays</b>	Saturdays, the two days of Rosh Hashana, Yom Kippur, the first day of Sukkot, Shmini Atzeret, the first and seventh day of Pesach, Independence Day, Shavuot, election days for the Knesset and local authorities.
<b>Cash Register Manufacturers</b>	An entity that develops or adapts cash register service software for Businesses, which includes management of the charges and credits

according to various Payment Methods, as well as management of inventory, promotions, connection to ERP systems, etc. The cash register software is connected to the Business's Terminal by a communications protocol and receives therefrom the daily credit card activity data.

<b>EMV Software Manufacturer/s</b>	An entity that develops software for Charge-Card Transaction Clearing based on a defined protocol, which is managed by the Protocol NGO and has received its approval for activity as a manufacturer of software for Clearing Transactions on the Payment System.
<b>System Rules / Rules</b>	These rules below, according to which the System is operated, including the annexes hereto.
<b>Collateral Funds</b>	Participants' funds which are deposited in the Clearing Account at the Central Bank and are used as collateral for any case of a failure event of a System Participant, to secure the daily Clearing. These funds shall be held in escrow by the System Operator for the benefit of the Participants for performance of the failure arrangement, including in any case of a failure event of a Participant.
<b>Smart Card</b>	A Charge Card that supports the EMV Standard.
<b>Clearing Failure</b>	"Financial Failure" and/or "Financial Operating Failure", as defined in Section 10.2 of the Rules.
<b>Aggregator</b>	As defined in Section 7B of the Banking Law (Customer Service), 5741-1981.
<b>Access Applicant</b>	An entity which has submitted an application to use the Payment System according to the directives of the Oversight of Payment Systems at the Bank of Israel.
<b>Payment Instruction Finality Date</b>	A date determined in the System Rules on which a transfer of a Payment Instruction is irreversible. The finality date is specified in the System Rules.
<b>Brand / Brands / International Organizations / International Schemes</b>	The international Charge Card organizations / brands that include the international organization Visa and/or the international organization Mastercard and/or the international organization American Express and/or the international organization Diners.
<b>Cleared Brand</b>	The Brands cleared by the relevant Acquirer.
<b>Card Holder</b>	A person for whose use a Charge Card was issued.
<b>Issuer</b>	An issuer, as defined in Section 11B of the Banking Law, and as amended in the Payment Services Law.

<b>Terminal / POS</b>	An electronic point of sale (POS) and payment system for the performance of charge-card Transactions at Businesses, which was approved for connection to the System by Shva.
<b>Approvals Interface Specification Document</b>	A document that describes the structure of Transaction Approval Request messages, the response to the Transaction Approval Request, and an advisory message (advice) transferred between the System and its Participants.
<b>RTGS System</b>	An RTGS (Real Time Gross Settlement) payment system for real-time same-day Clearing of payments, which is operated by the Bank of Israel according to the RTGS system rules, and constitutes a designated audited system as defined in the Payment Systems Law.
<b>Secure File Transfer System</b>	File transfers performed using secure systems such as safes.
<b>Retailers System</b>	A sub-system within the Payment System which manages the list of Terminals, the Parameters, Authorizations and Caps that the Acquirer seeks to allow for Terminal activity.
<b>Software Distributors</b>	An entity which markets to Businesses software of manufacturers of software for Charge-Card Transaction Clearing which is based on the EMV Protocol.
<b>System Operator / Payment System Operator</b>	As defined in the Payment Systems Law, and for purposes of these Rules – the Company is the system operator.
<b>Emergency Situation</b>	Any one of the following: a situation in which an emergency has been declared in Israel, declaration of a special situation on the home front pursuant to Section 9C of the Civil Defense Law, 5711-1951, or the declaration by the Supervisor of Banks of an emergency.
<b>Participant with Direct Technical Connection</b>	Type 1 Participants or Type 3 Participants, as specified in the Rules.
<b>System User</b>	Including the entities listed in Section 19 of the Rules, which are not System Participants.
<b>System Participant / Participant</b>	An Acquirer and/or Issuer and/or CLP Operator whose connection to the System has been approved by the Bank of Israel, which operates in the System according to the participation type as specified in Section 2.3.3.4 of the Rules.
<b>RTGS System Direct Participant</b>	A Participant having approval to participate in the RTGS System according to the RTGS System rules and which has a Clearing Account, and is able to receive and send Payment Instructions on

the RTGS System through the said account, as specified in and subject to the Rules and/or the annexes to the Rules.

**RTGS Clearing  
Represented  
Participant**

A Participant represented in the Settlement of the Net Results of the Charge-Card Payment System through an RTGS Representing Participant which is an RTGS System Direct Participant. The Settlement of the RTGS Clearing Represented Participant will be performed from the representative's Clearing Account, as specified in and subject to the Rules and/or the annexes to the Rules.

**Technical Connection  
Tier Represented  
Participant**

Type 2 Participants or Type 4 Participants, as specified in the Rules, which are represented in the technical connection tier in the System through a Technical Connection Tier Representing Participant, as specified in and subject to the Rules and/or the annexes to the Rules.

**Rules Represented  
Participant**

Type 3 Participants or Type 4 Participants, as specified in the Rules, which have not signed the System Rules, and are represented for purposes of the Rules through a Rules Representing Participant, as specified in and subject to the Rules and/or the annexes to the Rules.

**Rules Representing  
Participant / Rules-  
Tier Representing  
Participant**

A Participant which has signed the Rules also in connection with the activity of a Rules Represented Participant, as specified in and subject to the Rules and/or the annexes to the Rules. The Rules-Tier Representing Participant shall sign the Rules also on behalf of the Rules Represented Participant. The Rules Representing Participant shall be responsible for the Rules (including the annexes thereto), including in connection with the failure arrangement and completion of the Settlement in the RTGS System, also on behalf of the Rules Represented Participant.

**Technical Connection  
Tier Representing  
Participant**

A Participant with Direct Technical Connection, which has a technical connection to the System and meets the conditions for connection to the System, as specified in the Rules, which represents a Technical Connection Tier Represented Participant for the delivery of messages and interaction with the System. The Technical Connection Tier Representing Participant shall have a technical connection to the System also on behalf of the Technical Connection Tier Represented Participant, and shall deliver and receive messages and interact with the System on behalf of and for the Technical Connection Tier Represented Participant. The Technical Connection Tier Representing Participant shall be responsible for the activity of the Technical Connection Tier Represented Participant.

**RTGS Representing  
Participant**

An RTGS System Direct Participant which provides Settlement services to an RTGS Clearing Represented Participant through the Clearing Account of the RTGS Representing Participant. The Settlement activity of the RTGS Clearing Represented Participant will be part of the Clearing activity of the RTGS Representing



<b>Type 1-A Participant;</b> <b>Type 1-B Participant;</b> <b>Type 2-A Participant;</b> <b>Type 2-B Participant;</b> <b>Type 3 Participant;</b> <b>Type 4 Participant</b>	<p>Participant. An RTGS Representing Participant shall be responsible for Settlement for the RTGS Clearing Represented Participant.</p> <p>As specified in Section 2.3.3.4 of the Rules and subject to the Rules and/or the annexes to the Rules.</p>
<b>Represented Participant</b>	A Participant which is represented in the System through another System Participant, in one or more of the three access tiers: the Rules tier and/or the technical connection tier and/or the RTGS Clearing tier, as specified in and subject to the Rules and/or the annexes.
<b>Representing Participant</b>	A Rules-Tier Representing Participant and/or Technical Connection Tier Representing Participant and/or RTGS Representing Participant, as specified in and subject to the Rules and/or the annexes.
<b>CLP Operators</b>	A software company that provides payment services to private Brand Issuers, such as consumer programs, which allow closed-loop payment and benefit redemption.
<b>Point of No Return</b>	A point in time at which a Payment Instruction may no longer be canceled and/or modified by the System Participant.
<b>Acquirer</b>	As defined in the Banking Law.
<b>Settlement</b>	Execution of a Payment Instruction between one Participant and another Participant on the RTGS System (as defined in the RTGS System rules, as updated from time to time).
<b>Charge-Card Transaction Clearing</b>	As defined in Section 11(b) of the Banking Law.
<b>Clearing</b>	The process of transfer, adjustment, and in certain cases approval of Transactions prior to Settlement thereof, which may include netting of the Transactions and determines final Settlement balances.
<b>Interchange Fee</b>	The Issuer's fee which is collected from the Acquirer within the meaning thereof in the Banking Order (Customer Service) (Supervision of Charge Card and Debit Card Transaction Interchange Service), 5779-2018.

<b>Transactions / Entries / Underlying Transactions</b>	A Payment Instruction given by a Charge Card holder through a Business which was recorded by the Terminal.
<b>Special Transaction</b>	Any financial Entry which is not an Underlying Transaction that is entered into the System by a System Participant, such as: CHB (chargeback), REV (reverse chargeback), REP (representation).
<b>Personal Guarantee</b>	In any case of Clearing Failure, the System Operator shall cover the deficient amount to make up the Settlement of a failed direct Participant, through the Collateral Funds that such System Participant deposited in the Clearing Account of the System Operator, as specified in Section 10 of these Rules (the failure arrangement chapter).
<b>Mutual Guarantee</b>	In any case of Clearing Failure, the System Operator shall cover the deficient amount to make up the Settlement of a failed direct Participant, through the Collateral Funds deposited by the other direct System Participants in the Clearing Account of the System Operator, until the enactment of legislation on the issue, as specified in Section 10 of these Rules (the failure arrangement chapter).
<b>Oversight of Payment Systems</b>	The Oversight of Payment Systems Division in the Payment and Clearing Systems Department at the Bank of Israel.
<b>System's Core Activity</b>	The activity of the approvals and collection interface and/or the RTGS accounting and Clearing interface.
<b>Net Activity / Net Values / Net Results / Clearing</b>	The sum of the final balances for credit and/or debit between the System Participants in the context of the Settlement, as specified in the Rules.
<b>EMV Protocol</b>	A technological specification of a uniform and secure message structure developed based on the protocol of the International Schemes for Charge Cards and used for the transfer of approvals, Transactions and information between entities in the chain for the performance of charge-card Transactions in Israel in the segment between the Terminal and the Payment System.
<b>Parameters, Authorizations and Caps</b>	Characteristics at the Terminal level that are determined by the Acquirer, against which the Transaction is checked on the System.
<b>Pin-Pad</b>	Smart Card reader.
<b>AML Order</b>	An anti-money laundering order enacted by virtue of the Anti-Money Laundering Law, 5760-2000, which applies to the activity of the relevant entity.

<b>Blocked Cards File</b>	Files that include a list of Charge Cards that have been defined by the Participants as blocked (" <b>Blocked Cards</b> "), stating their block level.
<b>Blocked Cards File in the Terminal</b>	A file in the Terminal that contains a limited number of blocked Charge Cards according to the Terminals' capacity limit, according to the block levels determined by the System Participants.
<b>Input Control File</b>	A file which includes a specification of the Transactions / Entries denied by the accounting interface and the total number of Entries and amounts received by the accounting interface based on predetermined parameters.
<b>Monthly Balances File</b>	A file which contains Entries in a detailed credit and debit structure in respect of any Transaction / Entry for which no accounting was yet performed in the previous calendar month for any System Participant who is connected to the Transactions in the file.
<b>Usage File</b>	A file managed at the System Operator which contains data on the Transactions made on Charge Cards on the current Business Day and on three previous Business Days.
<b>Retailers File</b>	A file produced on an Acquirer level which contains a specification of all of the authorizations, caps and parameters for the Cleared Brands at the Terminal level. The file contains batch information on Terminals at the Businesses cleared by the Acquirer. The file contains all of the parameters and caps for each Brand.
<b>Multi-Beneficiary</b>	A Terminal used by a large number of Businesses. The Terminal transmits a batch of all of the Transactions, and the Acquirers / Aggregator credit each Business separately.
<b>Multi-Supplier</b>	A (central) master Terminal which aggregates several sub-terminals with different (Supplier) account numbers at the Acquirers. Each Supplier is credited separately.
<b>Informational Entry</b>	A non-financial Entry entered into the System by a Participant, such as: cancelation of a standing order.
<b>Caps</b>	The financial caps against which the sum of the Transaction is checked on the System. Determined at the Terminal level by the Acquirer.
<b>Transaction Approval Request</b>	A communication by a Terminal to the System for a transaction approval request.
<b>End-of-Day Communication</b>	A communication by a Terminal to the System to transmit Transactions and receive updates to Parameters, Authorizations and Caps.

<b>EMV / EMV Standard</b>	A Smart Card standard agreed upon by the International Organizations with the aim of providing a uniform and secure format for payment transactions using Charge Cards with a chip – Smart Cards, via an automated teller machine (ATM) or Terminal that support the standard (the standard is outlined in detail at: <a href="http://www.emvco.com">www.emvco.com</a> ).
<b>Payment Gateway</b>	Entities that supply technological infrastructure for Businesses, <i>inter alia</i> , services for the transfer of Transactions between Businesses and Acquirers or processors on their behalf. The service is mainly provided to Businesses that perform charge-card Transactions on the internet, and does not include handling the Clearing of the funds.
<b>Stand In Process (Stip)</b>	Providing a response to the Business on behalf of the System Participant according to a set of rules that were defined by the System Participant and were delivered in writing to the System Operator.

### 1.3. Objective and Purpose of the Rules

The objective and purpose of the Rules is to constitute a basis for regulation of the System's activity, including:

- 1.3.1. Ensuring its stability, efficiency and proper functioning.
- 1.3.2. Determination of rules regarding a Participant's participation, including:
  - 1) Fair System connection requirements of the applicants seeking to participate therein and non-discrimination between System Participants and applicants seeking to participate therein which have similar characteristics.
  - 2) Continued participation in the System by a Participant against which dissolution proceedings are being conducted.
  - 3) Means for enforcement of the rules.
- 1.3.3. Determination of adequate principles for cyber and information security, risk management and business continuity.
- 1.3.4. Determination of backup arrangements for emergencies.

### 1.4. The System Rules and the annexes thereto

These rules are "Charge-Card Payment System Rules". The annexes to these Rules are an integral part hereof.

### 1.5. Confidentiality of the Rules

- 1.5.1. These Rules, and any functional and/or technical and/or operating and/or any other information stated in these Rules, including the annexes thereto, and any information, details, documents, data or other material, whether in writing or oral, whether in electronic or other means, regardless of whether or not it is marked "confidential", which has reached or shall reach a System Participant in connection with its participation in the System and/or its activity and/or in connection with and/or as deriving from these Rules and/or performance hereof, is "confidential information",

and may be used by the System Participants and/or persons acting on their behalf for purposes of their activity in the System only.

- 1.5.2. The System Participants are required to keep the confidential information fully and absolutely confidential, and not to disclose, release or transfer the same to any third party without the prior written consent of the System Operator. Without derogating from the generality of the aforesaid, the System Participants undertake to take any and all precautions required to prevent the confidential information, in whole or in part, from leaving their possession and reaching any third party that is not authorized to receive the same, including taking the measures required for protection of confidentiality by their employees and/or persons acting on their behalf. A condition to the transfer of the Rules to a System Participant (or Access Applicant) is the signing, by the System Participant (or Access Applicant), of an NDA in the language attached hereto as Annex 2.

#### **1.6. Validity of the Rules**

The language of the Rules is updated from time to time according to the needs of the market, the needs of the System Participants, Statutory Requirements, the System Operator's discretion and for other reasons, all subject to the provisions of the law. The binding version of the Rules is the latest and most current version in Hebrew, of which the Bank of Israel is aware.

#### **1.7. Hierarchy**

- 1.7.1. In any case of discrepancy between the Payment Systems Law and the Rules – the provisions of the Payment Systems Law shall prevail.
- 1.7.2. In any case of discrepancy between the Rules and Statutory Requirements – the provisions of the Statutory Requirements shall prevail.
- 1.7.3. In any case of discrepancy between the Rules and the Agreements with the Participants – the provisions of the Rules shall prevail.
- 1.7.4. In any case of discrepancy between the provisions of the Rules and the provisions of the annexes to the Rules – the provisions of the Rules shall prevail.

#### **1.8. Roles, powers and the intellectual property of the System Operator**

- 1.8.1. Shva owns the rights in the System.
- 1.8.2. Shva is the operator of the System.
- 1.8.3. The work and services that have been carried out and/or provided and/or shall be carried out and/or provided and/or additional services, including future additional services, that have been and/or shall be provided to the System Participants, whether per the explicit request of the System Participants or the development and/or service was provided at Shva's initiative, and any product and/or development and/or intellectual property in connection with the System and/or technologies and/or systems and/or applications and/or software and/or products of Shva that were and/or shall be developed and/or were and/or shall be obtained and/or were and/or shall be discovered during the course of performance of the work and/or the services, will be the full and incontestable property of Shva, and neither the System Participants nor anyone on their behalf has or shall have any right therein.

### 1.9. Modification of the Rules

- 1.9.1. The System Operator may make, from time to time, improvements, amendments and/or modifications to the Rules and the annexes to the Rules, at its sole discretion.
- 1.9.2. However, and in order to preserve the transparency and fairness of the System Rules, no material and significant modification shall be made to the Rules other than after a discussion is held on the proposed modification in the Participants Committee or any other relevant forum, as shall be determined by the System Operator.
- 1.9.3. Where the modification shall affect a System Participant or certain Participants only, a discussion shall be held in connection with the proposed modification only with such System Participant or Participants regarding the planned modification to the Rules.
- 1.9.4. Where the proposed modification will affect all of the System Participants, a discussion shall be held with all of the System Participants, in the Participants Committee or any other relevant forum, as shall be determined by the System Operator.
- 1.9.5. The System Operator shall carefully review the implications of the modifications before making any modification.
- 1.9.6. The System Operator shall be exempt from consulting as aforesaid in urgent cases in which an immediate modification to the Rules is required and/or where the modification to the Rules is required due to Statutory Requirements.
- 1.9.7. Modification for purposes of this section includes the addition and/or removal of a System Participant.
- 1.9.8. Modifications to the Rules will be made by the System Operator only, unless stated otherwise in these Rules.
- 1.9.9. Modifications to the Rules which affect the operation or entail modification of the operating rules of another payment system will be made with the consent of the operator of the other payment system affected by the modification.
- 1.9.10. The System Operator shall report to the System Participants, through their representatives as specified in Annex 1 hereto, on the planned modifications to the Rules no later than 30 days before implementation of the modification. The aforesaid notwithstanding, where the modification to the Rules is required to be performed immediately, the System Operator shall report on performance of the modification to the System Participants as early as possible.

### 1.10. The Participants' entitlement to a copy of the Rules and receipt of information

- 1.10.1. After approval by the Bank of Israel and subject to the signing of a details form and an application to receive the System Rules for logon to the System, in the language attached hereto as Annex 1, and the signing of an NDA prior to delivery of the System Rules in the language attached hereto as Annex 2, the Company shall deliver a copy of the sensitive Rules to the Access Applicant seeking to be a System Participant.
- 1.10.2. The said System Participants shall be entitled to receive ongoing and periodic updates in connection with the System and the System Rules as is standard at the Company and at the Company's discretion. For receipt of additional information, the System Operator may be contacted according to the details stated in Section 1.12.1 of these Rules.

**1.11. Supplementary materials**

The Rules present the functional relationships between the System Participants and the System and the System Operator and between the System Participants among themselves. The System Participants must peruse other documents (such as specific specifications, file names, processes, etc.) which present the technical and operating activity of the System, as needed and relevant.

**1.12. Participants' communication with the System Operator**

1.12.1. Wherever these Rules require contacting the System Operator, for communication relating to participation in the System, use the following contact details:

Automatic Bank Services Ltd. (Shva)

26 Harokmim St., Holon

On technical support issues – contact the Support Department:

Tel: 03-5264666

E-mail: [support@shva.co.il](mailto:support@shva.co.il)

On other System-related issues – contact the Partner Relations Department:

E-mail: [Partner-Relations@shva.co.il](mailto:Partner-Relations@shva.co.il)

1.12.2. Any communication by a System Participant with the System Operator for the performance of an action relating to the System Participant's activity other than in the framework of the activity as defined in the Rules, shall be made in writing and delivered via e-mail and/or registered post, signed by an authorized representative on behalf of the communicating Participant.

1.12.3. A list of authorized representatives on behalf of the System Participant shall be delivered to the System Operator during its subscription to the System, via a form in its language as Annex 1 hereto. The System Participant is required to inform the System Operator of any change to the list of authorized representatives on behalf of the Participant, no later than 5 Business Days after the change takes effect.

1.12.4. Communication by the System Operator with the System Participants for the delivery of notices relating to the System's activity shall be made with the contact persons provided by the Participants, as specified in Annex 1 hereto.

**1.13. Backup systems and sites**

The backup sites and backup system are an integral part of the System, and the Rules apply to the backup sites and backup systems as they apply to the System.

**1.14. System operating room**

The Company has an operating / control room which operates around the clock, during routine times and emergencies, whose roles include:

- 1) Operating the processes on the relevant systems.
- 2) Control of activities of the infrastructures and the infrastructure systems.
- 3) Handling of failure events and referring the event to the responsible function as needed.
- 4) Reporting to the responsible functions upon the materialization of a failure event.
- 5) Handling of communications by Participants and users.

**Contact details:** 03-5264660 / 03-5264659.

## 1.15. Reporting on Irregular Events and Emergency Situations

### 1.15.1. Reporting on Irregular Events

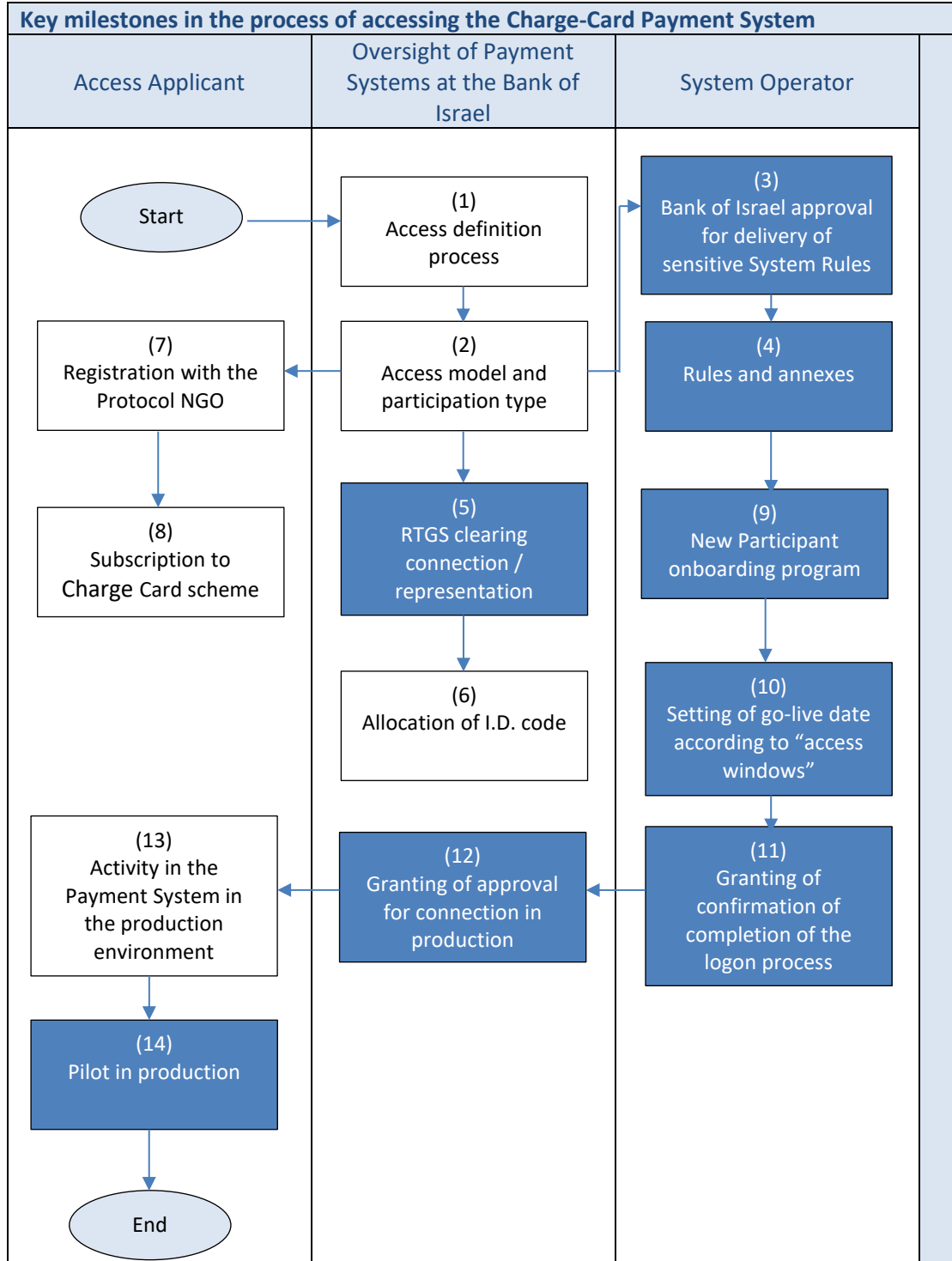
- 1) The System Participants are required to comply with Directive 2 of the Supervision Directives, and in this context the System Participants shall report to the System Operator, immediately and without delay, by telephone and in writing, on the materialization or any concern of the materialization of an Irregular Event, including but not limited to, the following events:
  - Communication problems or communication infrastructure outage that prevents the sending / receipt of instructions to/from the System;
  - Business / operating / infrastructure-related / app problems at the direct Participant or Represented Participant in the System which disrupts or may disrupt the System's activity;
  - Technical problems at the System Participant that prevent it from sending instructions to the System;
  - Any actual or suspected information security event or cyber attack on a System Participant;
  - The sending of an irregular number of instructions to the System by a System Participant;
  - A System Participant's failure to comply with the System Rules;
  - Receipt of a claim and/or class action against the System Participant;
  - Any occurrence of fraud and/or deception and/or willful sabotage by an employee vis-à-vis the System.
- 2) The reporting must be immediate and no later than the end of the Banking Business Day on which the event occurred or became known.
- 3) Participants with a direct technical connection to the System are responsible for reporting any concern or materialization of an Irregular Event experienced by them and/or one or more of the Participants represented in the technical tier through them, where the concern or event affect the System's activity.
- 4) The report shall include a specification about the event, its repercussions, etc., as specified in Annex 14 hereto.
- 5) A detailed 'lessons learned' report about the Irregular Event shall be submitted no later than 30 Business Days after the date of the immediate report on the Irregular Event, according to the specification in Annex 15 hereto.
- 6) Insofar as there is no legal impediment and the System Operator deems it justified to report on the materialization of an Irregular Event to all of the System Participants, no breach of confidentiality vis-à-vis other Participants shall be implied thereby.



## 2. System Access and Participation Types

### 2.1. Key milestones in the process of accessing the System

Process diagram:



**Explanation of the process:**

#	Milestone	Description	Responsible entity	Relevant entity
1	<b>The process for defining access to the Payment System</b>	Introductory conversation with the Oversight of Payment Systems. As specified in Section 2.2 of these Rules.	Access Applicant	Oversight of Payment Systems
2	<b>Defining access models and participation type</b>	The Access Applicant shall define the type of its System participation in each one of the System access tiers. As specified in Section 2.3 of these Rules.	Access Applicant	Oversight of Payment Systems
3	<b>Bank of Israel approval for delivery of sensitive System Rules</b>	Granting of approval for delivery of sensitive System Rules.	Oversight of Payment Systems	System Operator
		The sensitive System Rules shall be delivered to the Access Applicant after receipt of a details form and an application to receive the System Rules for subscription to the System and an NDA – prior to delivery of the System Rules as specified in Section 2.5 of these Rules.	Access Applicant	System Operator
4	<b>Signing of System Rules and/or annexes</b>	Signing of the System Rules document and the annexes thereto. As specified in Section 2.6 of these Rules.	Access Applicant	System Operator
5	<b>RTGS Clearing connection / representation</b>	Deciding whether to be an RTGS Clearing Represented Participant through an RTGS Clearing Representing Participant or an RTGS System Direct Participant. As specified in Section 2.7 of these Rules.	Access Applicant	RTGS System operator / RTGS Clearing representing Participant
6	<b>Allocation of I.D. code</b>	The Access Applicant shall comply with the I.D. code policy posted on the Bank of Israel website <a href="https://www.boi.org.il">https://www.boi.org.il</a> As specified in Section 2.8 of these Rules.	Access Applicant	Oversight of Payment Systems
7	<b>Registration with the Protocol NGO</b>	Registration with the Protocol NGO and receipt of the protocol. As specified in Section 2.4 of these Rules.	Access Applicant	Protocol NGO
8	<b>Subscription to Charge Card scheme</b>	Subscription to Charge Card scheme. As specified in Section 2.9 of these Rules.	Access Applicant	System Operator
9	<b>New Participant onboarding</b>	The System Operator shall set timetables with the Access Applicant	System Operator	Access Applicant

	<b>program – direct technical connection</b>	for the logon process, including delivery of System documentation, completion of developments, tests and integration. As specified in Section 2.10 of these Rules.		
<b>10</b>	<b>Go-live date according to “access windows”</b>	The Access Applicant shall coordinate the go-live date with the System Operator. As specified in Section 2.11 of these Rules.	Access Applicant	System Operator
<b>11</b>	<b>Confirmation of completion of the logon process</b>	Granting of confirmation of completion of development, QA and integration tests. As specified in Section 2.12 of these Rules.	System Operator	Oversight of Payment Systems
<b>12</b>	<b>Granting of approval for connection in production</b>	Granting of approval for commencement of activity in the production environment. As specified in Section 2.13 of these Rules.	Oversight of Payment Systems	System Operator
<b>13</b>	<b>Activity in the Payment System in the production environment</b>	Commencement of the new Participant’s activity in the Payment System in the production environment.		
<b>14</b>	<b>Pilot in production</b>	Gradual and limited activity by the new Participant in the production environment of the Payment System. As specified in Section 2.14 of these Rules.	Access Applicant	System Operator

## 2.2. Defining the access to the Payment System

- 2.2.1. **Access conditions and methods** are determined by the Oversight of Payment Systems at the Bank of Israel and are specified in the Payment System Access Guidelines as released by the Bank of Israel<sup>2</sup> and/or another relevant document that shall replace it, as shall be released by the Bank of Israel.
- 2.2.2. The Access Applicant may hold an introductory conversation with the Oversight of Payment Systems to ascertain its needs and for information on the participation types relevant to its activity in the System.

---

<sup>2</sup> [Access to audited and designated audited payment systems | Bank of Israel – the Central Bank of the State of Israel \(boi.org.il\)](https://www.boi.org.il/Access%20to%20audited%20and%20designated%20audited%20payment%20systems%20-%20Bank%20of%20Israel%20-%20the%20Central%20Bank%20of%20the%20State%20of%20Israel%20(boi.org.il).).

- 2.2.3. The Access Applicant is required to obtain the approval of the Oversight of Payment Systems for its connection to the Payment System, directly or through a representing Participant in each one of the three access tiers (jointly or severally).
- 2.2.4. The Access Applicant is an entity whose subscription to the Payment System the System Operator may allow according to Statutory Requirements and/or the Access Applicant's license (including an Access Applicant that is in the process of obtaining an appropriate license as foresaid).
- 2.2.5. The Access Applicant meets the eligibility conditions and proceedings for connection, as specified in these Rules.

### 2.3. Access models and participation type

- 2.3.1. Access to the Payment System is divided into three tiers. Each tier provides two options and the combination of any one of the options in all of the three tiers constitutes an **access model** ("**Participation Type**"), as specified below:

Tier	Participation Type	Description
Rules	<b>Rules direct Participant</b>	Has signed the System Rules.
	<b>Rules Represented Participant</b>	Has not signed the System Rules and is represented in the Rules through a Rules Representing Participant.
Technical connection	<b>Technical connection direct participant</b>	A Participant with direct technical connection to the System (meets the connection requirements).
	<b>Technical Connection Tier Represented Participant</b>	A Technical Connection Tier Represented Participant which has a technical connection to the System through another Technical Connection Tier Representing Participant.
RTGS Clearing	<b>RTGS System Direct Participant</b>	An RTGS System Direct Participant which clears its activity on the Charge-Card Payment System through its Clearing Account.
	<b>RTGS Clearing Represented Participant</b>	An RTGS Clearing Represented Participant which clears its activity on the charge-card system through a Clearing Account of an RTGS System Direct Participant (RTGS Representing Participant).

#### 2.3.2. Threshold conditions for technical connection

- 1) Existence of internal procedures and/or instructions at the Access Applicant, for purposes of work vis-à-vis the System, including according to the provisions of the Rules. In any case of discrepancy between the internal procedures and/or instructions of the Access Applicant and these Rules, the provisions of these Rules shall prevail (also after the Access Applicant becomes a System Participant).
- 2) The Access Applicant (and subsequently the System Participant) is required to:
  - 2.1) Have required technological capabilities that allow it to comply with these Rules, including building a secure communication infrastructure with high

survivability for connection of the Access Applicant and as specified in these Rules.

- 2.2) Comply with the information security requirements presented in Section 13 below.
- 2.3) Comply with the business continuity conditions presented in Section 15 below, including adequate backup arrangements which will not impact the System's regular activity.
- 2.4) Comply with any other requirement stated in the System Rules.

#### **2.3.3. Participation Types**

- 2.3.3.1. According to Directive 10 of the Supervision Directives, based on Principle 18 of the PFMI, a system operator is required to define in the system rules all types of participation in the system according to each type of activity in the system, as well as the connection requirements for each participation type as aforesaid.
- 2.3.3.2. The System Operator shall determine additional requirements for Participants that rely on the services of other Participants, if it deems fit, to ensure their proper activity in the System.
- 2.3.3.3. The Access Applicant shall define its requested type of participation in the System in each one of the three tiers specified above.
- 2.3.3.4. According to the aforesaid, presented below are the relevant types of participation in the System:

Type/tier	Rules		Technical connection		RTGS Clearing		Type of responsibility borne by the Participant	Type of responsibility borne by the Participant's representative
Participant type	Direct – has signed the Rules	Represented – has not signed the Rules	Connected	Not connected	Direct Clearing Participant	Represented Clearing Participant	It is clarified that the provisions of this column supplement the provisions of Section 18 of the Rules	It is clarified that the provisions of this column supplement the provisions of Section 18 of the Rules
<b>1-A – Direct - Rules, technical connection and RTGS Clearing</b>	V		V		V		Full responsibility (including financial and operating) for its activity including the Settlement and/or the RTGS System Clearing activity, and for the activity of a Participant it represents in one or more of the access tiers in which it is a representative	N/A
<b>1-B – Direct - Rules and technical connection; Represented - RTGS Clearing</b>	V		V			V	Full responsibility (including financial and operating) for its activity and for the activity of a Participant it represents in one or more of the access tiers in which it is a representative	The RTGS Clearing tier Representing Participant bears full responsibility (including financial and operating) for the Settlement and/or the RTGS System Clearing activity for this Participant
<b>2-A – Direct - Rules; Represented - technical connection; Direct - RTGS Clearing</b>	V			V	V		Full responsibility (including financial and operating) for its activity including the Settlement and/or the RTGS System Clearing activity, and for the activity of a Participant it represents in one or more of the access tiers in which it is a representative	The Technical Connection Tier Representing Participant bears full responsibility (including financial and operating) in connection with the activity of this Participant in this tier

<b>2-B – Direct - Rules; Represented - technical connection and RTGS Clearing</b>	V			V		V	Full responsibility (including financial and operating) for its activity and for the activity of a Participant it represents in the Rules tier	<p>The Technical Connection Tier Representing Participant bears full responsibility (including financial and operating) in connection with the activity of this Participant in this tier</p> <p>The RTGS Clearing tier Representing Participant bears full responsibility (including financial and operating) for the Settlement and/or the RTGS System Clearing activity for this Participant</p>
<b>3 – Represented - Rules; Direct - technical connection; Represented - RTGS Clearing</b>		V	V			V	Full responsibility (including financial and operating) for its activity and for the activity of a Participant it represents in the technical connection tier	<p>The Rules-Tier Representing Participant bears full responsibility (including financial and operating) in connection with the activity of this Participant in this tier</p> <p>The RTGS Clearing tier Representing Participant bears full responsibility (including financial and operating) for the Settlement and/or the RTGS System Clearing activity for this Participant</p>

<p><b>4 – Represented - Rules, technical connection and RTGS Clearing</b></p>		<p>V</p>		<p>V</p>		<p>V</p>	<p>The Representing Participant shall bear the responsibility</p>	<p>The Rules-Tier Representing Participant bears full responsibility (including financial and operating) in connection with the activity of this Participant in this tier</p> <p>The Technical Connection Tier Representing Participant bears full responsibility (including financial and operating) in connection with the activity of this Participant in this tier</p> <p>The RTGS Clearing tier Representing Participant bears full responsibility (including financial and operating) for the RTGS System Clearing activity of this Participant</p>
---	--	----------	--	----------	--	----------	---	---



- 2.3.3.5. The System Participant that represents a Represented Participant (including a Type 4 System Participant) shall fill in and sign a confirmation of engagement in an agreement thereof as a representative with a Represented Participant in the System in the language attached hereto as Annex 8, as a condition to its activity as a representative in the System in one or more of the access tiers.
- 2.3.3.6. The System Participant that represents a Represented Participant (including a Type 4 System Participant) in one or more of the access tiers shall be responsible for and shall ensure fulfillment by the said Represented Participant of its commitment to cyber and information security and business continuity standards, according to the Statutory Requirements that apply to such Participant.

#### 2.4. Registration with the Protocol NGO

- 2.4.1.1. Access Applicants seeking to operate in the System as a Type 1 or Type 2 Participant (as defined above) are required to contact the Protocol NGO for their registration with the NGO and receipt of the EMV Protocol which is required for the process of connection to the Payment System.

#### 2.5. Bank of Israel approval for the delivery of sensitive System Rules to Access Applicants

- 2.5.1. The Oversight of Payment Systems at the Bank of Israel shall authorize the System Operator in writing to commence the subscription process vis-à-vis the Access Applicant.
- 2.5.2. After receipt of the authorization from the Oversight of Payment Systems at the Bank of Israel as aforesaid, the Access Applicant shall deliver to the System Operator a details form and an application to receive the System Rules for logon to the System as specified in Annex 1 to these Rules, and an NDA as specified in Annex 2 to these Rules, both signed by an authorized signatory of the Access Applicant.
- 2.5.3. The System Operator shall deliver to the Access Applicant the sensitive System Rules within 5 Business Days from the date of receipt of the above documents, signed to its satisfaction.

#### 2.6. Rules and annexes

- 2.6.1. Prior to initialization of the process of logon to the System and/or the activity in the System, the Access Applicant is required to review, fill in and sign the System Rules, including the annexes thereto, as specified below.
- 2.6.2. **No Participant shall use the System unless it has signed the System Rules, including the annexes thereto that are relevant to its participation type, in the standard language at the System Operator and to the System Operator's satisfaction, as specified below.**
- 2.6.3. Below is a table specifying the annexes that are relevant to each type of System Participant and/or RTGS Clearing representing Participant:

Annex no.	Annex name	Requirement	Type 1-A, 1-B Participant	Type 2-A, 2-B Participant	Type 3 Participant	Type 4 Participant
1	Details form and application to receive the System Rules for logon to the System	Fill in details and sign	V	V	V	V
2	NDA – prior to delivery of the System Rules	Fill in details and sign	V	V	V	V
3	List of contact persons for representation in the Payment System access models	FYI	V	V	V	V
4	Agreement between the System Operator and Type 1-A Participants or Type 1-B Participants	Fill in details and sign	V			
5	Agreement between the System Operator and Type 2-A Participants or Type 2-B Participants	Fill in details and sign		V		
6	Agreement between the System Operator and Type 3 Participants	Fill in details and sign			V	
8	Confirmation by representative of representation of a Represented Participant in the System	Fill in details and sign (insofar as relevant)	V	V	V	V
9	Form for customer onboarding by the System Operator	Fill in details and sign	V	V	V	V
10	List of Charge-Card Payment System Participants	FYI	V	V	V	V
11	Payment System failure arrangement, including the annexes thereto	FYI and fill in details and sign	V	V	V	V
12	Access Applicant's declaration to the System Operator regarding compliance with cyber and	Fill in details and sign	V	V	V	V

Annex no.	Annex name	Requirement	Type 1-A, 1-B Participant	Type 2-A, 2-B Participant	Type 3 Participant	Type 4 Participant
	information security requirements					
13	Access Applicant's declaration to the System Operator regarding compliance with business continuity requirements	Fill in details and sign	V	V	V	V
14	Notice of an Irregular Event which requires reporting	Format for reporting insofar as required	V	V	V	V
15	Notice of lessons learned from Irregular Event	Format for reporting insofar as required	V	V	V	V

## 2.7. RTGS System connection / representation

- 2.7.1. System Participants or Access Applicants wishing to be RTGS System participants shall comply with the access conditions and requirements for connection of nonbank payment service providers to the RTGS System posted on the Bank of Israel website at: [www.boi.org.il](http://www.boi.org.il).
- 2.7.2. A Participant or Access Applicant that wishes to be a RTGS Clearing Represented Participant ("**RTGS Representation Applicant**") shall comply with the directive on mandatory Clearing representation of the Oversight of Payment Systems of 29 October 2024 (or any other current instruction / directive of the Oversight of Payment Systems, as shall be released) (the "**Directive on Mandatory Clearing Representation**").
- 2.7.3. The RTGS Representation Applicant shall contact, in writing, one of the System Participants that manage a Clearing Account in the RTGS System, according to the list of contact persons as specified in Annex 3 to these Rules.
- 2.7.4. **Mandatory RTGS Clearing representation**
- 2.7.4.1. Mandatory RTGS Clearing representation and the conditions for obtaining RTGS System Clearing representation shall apply according to the provisions of the law (and specifically according to the Directive on Mandatory Clearing Representation). A System Participant that manages a Clearing Account in the RTGS System that received a representation application ("**Participant that Received a RTGS Clearing Representation Application**") is required to provide RTGS System Clearing representation to a Charge-Card Payment System Participant according to the provisions of the law and the provisions below. It is clarified that the duty applies where the applicant requests Clearing representation for its activity on the System for the provision of payment services to its customers, and not where the representation is intended for another purpose.

**2.7.5. Process of obtaining RTGS Clearing representation**

- 2.7.5.1. The Clearing representation applicant shall apply in writing to a System Participant that manages a Clearing Account in the RTGS System, for the receipt of Clearing representation services on the Charge-Card Payment System.
- 2.7.5.2. A Participant that Received a RTGS Clearing Representation Application shall give written notice<sup>3</sup> thereof to the System Operator, the Oversight of Payment Systems and the regulator thereof and the regulator of the Clearing representation applicant.
- 2.7.5.3. A Participant that Received a RTGS Clearing Representation Application shall give the RTGS Representation Applicant, the System Operator, the Oversight of Payment Systems, the regulator thereof and the regulator of the RTGS Representation Applicant, a response to such application within 30 Business Days, together with the representation requirements and conditions or reasons if it refuses the application. The said 30 days shall be counted from the date of submission of the representation application by the RTGS Representation Applicant or from the date of receipt of the sensitive Rules thereby, according to the access diagram released by the Oversight of Payment Systems, whichever is later.
- 2.7.5.4. In the event that the representation application is approved, the Participant that Received a RTGS Clearing Representation Application is required to complete the process of signing the Clearing representation annex according to the Rules vis-à-vis the System Operator within the said 30 Business Days (Annex 8 to the Rules).
- 2.7.5.5. A Participant that Received a RTGS Clearing Representation Application may charge fees for the representation service, which must be reasonable according to the characteristics of the service. The pricing will be, *inter alia*, risk-based and shall not restrict the ability of the RTGS Representation Applicant to receive representation or prejudice fair competition.
- 2.7.5.6. A Participant that Received a RTGS Clearing Representation Application shall specify the pricing of the costs deriving from provision of the representation services to the RTGS Representation Applicant.
- 2.7.5.7. In the agreement vis-à-vis the RTGS Representation Applicant, a Participant that Received a RTGS Clearing Representation Application may determine tools that will allow it to manage the risks entailed by the representation,

---

<sup>3</sup> Notices and updates to the Oversight of Payment Systems shall be via e-mail to [payments-oversight@boi.org.il](mailto:payments-oversight@boi.org.il). Notices to regulators and the system operators shall be given via e-mail to the addresses specified in Annex A and Annex B, respectively, to the Access Guidelines released by the Bank of Israel, the link to which appears in the Directive on Mandatory Clearing Representation.

including determining and using controls on various issues, and *inter alia* on money laundering and terror financing<sup>4</sup>, information security, etc.

2.7.5.8. A Participant that Received a RTGS Clearing Representation Application is required to complete the legal preparations and the signing of a representation agreement, as well as the operating preparation required for the representation, within a reasonable period of time which shall be no longer than three months, which shall be completed prior to commencement of the trial environment testing required for the Participant applying for Clearing representation to go live, according to the access window coordinated vis-à-vis the System Operator (it is clarified that the 30 days stated in Section 2.7.2.2.3 shall not be counted in the three months stated in this section). Non-compliance with the said timetables may lead to postponement of the access window coordinated vis-à-vis the System Operator.

2.7.5.9. After receipt of written in-principle approval from the RTGS Clearing Representing Participant and from the Oversight of Payment Systems at the Bank of Israel regarding the representation of the Represented Participant, the RTGS Clearing Representing Participant shall confirm vis-à-vis the System Operator that it bears full and sole responsibility for the risks that the RTGS Clearing Represented Participant transfers to the System and/or full financial and operating responsibility for its RTGS Clearing activity with respect to the Represented Participant's activity in the System, according to the provisions of Annex 8 to the Rules. The RTGS Clearing Representing Participant shall deliver to the System Operator a full and signed copy of Annex 8 to these Rules, as a condition to its activity as a RTGS Clearing representing Participants in the Charge Card system.

#### 2.7.6. Refusal to represent

2.7.6.1. A Participant that Received a RTGS Clearing Representation Application shall not unreasonably refuse to provide RTGS Clearing representation to a System Participant or Access Applicant wishing to be a RTGS Clearing Represented Participant.

2.7.6.2. A Participant that Received a RTGS Clearing Representation Application shall not impose unreasonable conditions on Clearing representation.

2.7.6.3. Examples of reasonable refusal to provide Clearing representation:

---

<sup>4</sup> The aforesaid does not imply that the Participant that received a representation application is responsible for preventing money laundering and terror financing committed through the RTGS Representation Applicant. The Participant that Received a RTGS Clearing Representation Application is required to comply with the regulation that applies thereto on the issue, and may perform various AML controls, such as monitoring irregularities in the net Clearing of the RTGS Representation Applicant which may be questionable.

2.7.6.3.1. Non-compliance by a System Participant and/or Access Applicant as aforesaid seeking representation services with one of the following conditions:

- (a) The System Participant and/or Access Applicant as aforesaid does not meet the AML Order or the AML Order does not apply thereto;
- (b) The Participant and/or Access Applicant as aforesaid does not implement tools that were reasonably required by the RTGS Clearing Representing Participant for management of the risks entailed by the representation and according to the Statutory Requirements that apply to the RTGS Clearing Representing Participant, including presentation of documents and approvals required for such purpose.
- (c) Special circumstances relating to the RTGS Clearing Representing Participant, including scope of activity and fields of activity.

2.7.6.3.2. Insofar as the RTGS Clearing Representing Participant refuses an application, the representation applicant may approach the Oversight of Payment Systems if it believes that the refusal was unreasonable. Should the Oversight of Payment Systems find that the refusal of the RTGS Clearing Representing Participant was indeed unreasonable, it will be given a right to present its arguments and reconsider its response. Where the Oversight of Payment Systems believes that the refusal is unreasonable, this may amount to non-compliance with the System Rules and a breach of the duty of representation.

#### **2.7.7. Termination of representation at the initiative of a RTGS Representing Participant**

2.7.7.1. In any case where the RTGS Clearing Representing Participant seeks to terminate an engagement with a Clearing Represented Participant, the RTGS Clearing Representing Participant is required to inform the Clearing Represented Participant, by giving prior written notice of at least 120 days in advance, in order to enable it to engage with another alternative representing Participants.

2.7.7.2. Upon provision of the RTGS Clearing Representing Participant's notice of termination of the representation, including giving reasons for termination of the representation, the Representing Participant shall notify the System Operator, the Oversight of Payment Systems and the regulator thereof and of the RTGS Clearing Represented Participant of the decision.

2.7.7.3. The RTGS Clearing Represented Participant may approach the Oversight of Payment Systems if it believes that the reason for termination of the representation is unreasonable. Should the Oversight of Payment Systems find that the RTGS Clearing Representing Participant did indeed give an unreasonable reason for termination of representation, the RTGS Clearing Representing Participant shall be given a right to present its arguments and reconsider its decision. Where the Oversight of Payment Systems believes that the representation was unreasonably terminated, this may amount to

non-compliance with the System Rules and a breach of the duty of representation.

2.7.7.4. Insofar as the RTGS Clearing Represented Participant is entitled to continue using the Payment System, it is responsible for taking action to engage with another alternative RTGS Representing Participant, or connecting as a RTGS System Direct Participant, according to the provisions of Section 2.7.1 of the Rules above.

**2.7.8. Termination of representation at the initiative of a RTGS Clearing Represented Participant**

2.7.8.1. In any case where the RTGS Clearing Represented Participant seeks to terminate an engagement with a RTGS Clearing Representing Participant, the Clearing Represented Participant is required to inform the RTGS Clearing Representing Participant, by giving prior written notice of at least 60 days in advance.

2.7.8.2. Insofar as the RTGS Clearing Represented Participant is entitled to continue using the Payment System, it is responsible for taking action to engage with another alternative RTGS Representing Participant, or connecting as a RTGS System Direct Participant, according to the provisions of Section 2.7.1 of the Rules above.

**2.7.9. Cancellation / suspension of a Clearing Represented Participant at the System Operator's initiative**

2.7.9.1. In any case of a decision to suspend or cancel the suspension or cancel the participation of an RTGS Clearing Represented Participant in the Payment System, the System Operator shall take action according to the provisions of Section 11 of the Rules in this regard.

2.7.9.2. In any case of suspension or cancelation of the suspension or cancelation of the participation of a Clearing Represented Participant in the Payment System, the RTGS Representing Participant is responsible for making preparations for termination or renewal of the Clearing in practice, without prejudice to the existing current processes. For example: continued activity of the System without receipt of a Clearing file for the said Participant or receipt of an empty file.

**2.8. Allocation of I.D. code – Bank of Israel**

2.8.1. The Access Applicant shall submit an application to the Oversight of Payment Systems for receipt of an I.D. code according to the I.D. code policy, as determined by the Bank of Israel and posted on the Bank of Israel website – <https://www.boi.org.il>.

**2.8.2. Clarifications for the process vis-à-vis the System Operator:**

2.8.2.1. The System Operator's confirmation that an application to participate in the System has been received shall be granted after receipt of a details form and an application for receipt of the System Rules for logon to the System (in the language attached to the Rules as Annex 1) and an NDA – prior to delivery of the System Rules (in the language attached to the Rules as Annex 2), filled in and signed by the Access Applicant to the System Operator's satisfaction;

2.8.2.2. Insofar as the Access Applicant is not an RTGS Clearing direct Participant (but rather is represented through an RTGS Clearing Representing Participant),



the Access Applicant shall deliver to the Oversight of Payment Systems at the Bank of Israel confirmation regarding RTGS Clearing representation, approved and signed by the RTGS Clearing Representing Participant (in the language attached to these Rules as Annex 8).

## 2.9. Subscription to Charge Card scheme

- 2.9.1. On 17 July 2024, the Bank of Israel declared the Payment System – Charge Card Scheme (formerly known as the “local agreement”) a controlled system, and Shva – a Charge Card scheme system operator.
- 2.9.2. A Charge Card scheme (the local agreement) is a contractual system which regulates the financial accounting rules and the handling of transactions between Acquirers and Issuers in connection with their Charge Card activity, including: setting dates for accounting in respect of Transactions, rates, indices, charge backs, etc.
- 2.9.3. Subscription by Access Applicants which are Acquirers / Issuers to the scheme constitutes a condition to the Payment System going live.
- 2.9.4. The Access Applicant is responsible for submitting to Shva a scheme subscription application.

## 2.10. New Participant onboarding plan – direct technical connection

### General

- 2.10.1. The System Operator, the Access Applicant and the System Participants shall act according to the new Participant onboarding plan, including the developments, the tests and the dates for performance thereof, until completion of the go-live in production. The process shall include both tests vis-à-vis the operator and integration tests vis-à-vis all of the System Participants, including other users operating in the transaction chain.
- 2.10.2. The System Operator shall determine timetables with the Access Applicant for the logon process, including delivery of System documentation, completion of developments, tests and integration and a go-live date in these Rules.
- 2.10.3. All of the System Participants and/or the users operating throughout the transaction chain are responsible for enabling the joining of a new Participant in a manner that allows it to conduct adequate end-to-end operations according to reasonable timetables that shall be **no longer than 3 months** from the date of the System Operator’s notice regarding the go-live date.
- 2.10.4. In addition, but not only, it is the responsibility of each System Participant which is an **Acquirer** to ensure that all of the Aggregators operating through it, and each user which is an **EMV Software Manufacturer** to ensure that all of the distributors and Cash Register Manufacturers that operate in collaboration therewith, and any other entity that operates in the transaction chain, receive and comply with the guidelines detailed in the New Participant Onboarding Plan. It is clarified that System Participants and/or users, including but not limited to the entities operating in a transaction performance chain, that do not support end-to-end activity of new Participants, will be acting contrary to the criteria of the EMV Standard, and contrary to agreements reached by the payments market in Israel regarding the connection of new Participants and/or new users. Therefore, in this case, such entities may be in breach of the EMV Standard and will not be permitted to use the Payment System.



- 2.10.5. An Access Applicant which is an Issuer shall deliver to the System Operator a specification of the prefixes of the Charge Cards issued and/or marketed and/or distributed thereby, the types of the said Charge Cards and the manner of testing thereof in the System and in the Terminals.
- 2.10.6. Insofar as an existing System Participant or the Access Applicant will engage in an agreement with a technical tier Represented Participant, which is supposed to rely on the services of the System Participant or Access Applicant, the System Participant or Access Applicant shall provide the System Operator with any relevant information regarding the technical tier Represented Participant which the System Operator shall request, including, and without derogating, a specification of the prefixes of the Charge Cards issued and/or marketed and/or distributed by the Represented Participant, the types of the said Charge Cards and the manner of testing thereof in the System and in the Terminals, and any other information regarding the technical tier Represented Participant that the System Operator shall request which is required for its activity in the System.

#### **Delivery of documentation**

- 2.10.7. After delivery of the annexes required of an Access Applicant, filled in and signed to the System Operator's satisfaction, the System Operator shall deliver to the contact person on behalf of the Access Applicant seeking to be a Type **1 or 3** Participant with Direct Technical Connection, the relevant documents according to the type of its activity in the System.
- 2.10.8. **System documentation for a System Participant that is an Acquirer**

#	Package	Description
1	<b>General</b>	Top-level specification for subscription by a new Acquirer to the Payment System
2	<b>Switch connection</b>	Specification of a TCP/IP connection to the Payment System switch
3	<b>Approvals interface</b>	Specification of OL approvals interface – approval application process
4		Specification of messages between the credit card companies
5	<b>Terminals and authorizations</b>	Structure of file of applications for approval of Terminals for credit card companies
6		Opening and updates structure
7		Denials file structure
8		Terminals charging control file structure
9		Clearing endorsements interface structure
10		Endorsements error structure
11		Retailers File structure
12	<b>Transactions interface</b>	Structure of transactions file for Acquirer
13		Structure of gross transactions file for Acquirer
14	<b>Accounting interface</b>	Functional specification file
15		Files planning document – accounting interface files
16		Adequacy testing document
17		General specification for changes to the Clearing interface system
18	<b>Tests and integration</b>	Specifications of tests and/or testing instructions that are adapted to the basic services and other information details in

		connection with the work of the Access Applicant seeking to be an Acquirer-type Participant in the System, vis-à-vis the System
--	--	---

#### 2.10.9. System documentation for a System Participant that is an Issuer

#	Package	Description
1	<b>General</b>	Top-level specification for subscription by a new Issuer to the Payment System
2	<b>Switch connection</b>	Specification of a TCP/IP connection to the Payment System switch
3	<b>Approvals interface</b>	Specification of OL approvals interface – approval application process
4		Structure of the online messages for the transfer of OL blocked cards and specification of Blocked Cards File structure
5	<b>Accounting interface</b>	Functional specification file
6		Files planning document – accounting interface files
8		Adequacy testing document
9		General specification for changes to the Clearing interface system
10	<b>Loyalty programs interface</b>	Structure of loyalty program agreements file
11		Structure of file of cards entitled to loyalty program discounts
12	<b>Tests and integration</b>	Specifications of tests and/or testing instructions that are adapted to the basic services and any other information required for its work vis-à-vis the System

#### 2.10.10. System documentation for a System Participant that is a CLP Operator

#	Package	Description
1	<b>Switch connection</b>	Specification of a TCP/IP connection to the Payment System switch
2	<b>Terminal management</b>	Specification of Terminal opening and management interface
3	<b>Approvals interface</b>	Specification of OL approvals interface – approval application process

#### Technical connection

2.10.11. The requirements for connection to the Payment System are determined by the System Operator, and they include the technological, operating and business requirements for participation in the System.

2.10.12. The System Operator and the System Participants shall comply with this plan, including the developments, the tests and the dates for performance thereof, until completion of the go live in production. The process shall include both integration tests vis-à-vis the operator and end-to-end tests vis-à-vis all of the System Participants.

2.10.13. The Access Applicant is required to notify the System Operator as early as possible of any material change in the eligibility conditions and its compliance with the eligibility conditions specified in these Rules.

- 2.10.14. The technical representative on behalf of the Access Applicant, as specified in the logon application form, shall contact the System Operator for receipt of explanations and coordination of all of the technical aspects required for the Access Applicant's logon to the System, insofar as required, by the Access Applicant.
- 2.10.15. Insofar as the Access Applicant is so required by the System Operator, it shall perform developments and adjustments in its systems in order to render them compatible with logon to the System, and shall ensure they are compliant with the requirements.
- 2.10.16. Insofar as required, the System Operator shall perform developments and adjustments in its systems to onboard and integrate the Access Applicant in the Payment System.

#### **Information security survey**

- 2.10.17. The Payment System is a critical state infrastructure, and therefore an Access Applicant seeking to have a direct technical connection to the System is required to undergo a YUVAL survey examination by a surveyor authorized by the National Cyber Directorate.
- 2.10.18. The Access Applicant is responsible for taking action for performance of the survey at its expense prior to completion of its connection to the Payment System, including addressing the findings, if any.

#### **Tests and integration**

- 2.10.19. Prior to commencement of the tests, the Access Applicant is required to meet the eligibility requirements specified in these Rules; it is clarified that it is the System Operator that is authorized to determine, at its sole discretion, whether the Access Applicant does indeed meet the eligibility requirements specified above.
- 2.10.20. The Access Applicant shall notify the System Operator in writing that it has performed the tests required by the directives delivered thereto and of its readiness to perform the testing with the System Operator.
- 2.10.21. The tests shall be carried out according to the testing specifications in the book of tests delivered to the Access Applicant by the System Operator. Insofar as the System Operator believes it to be necessary, some of the tests that the Access Applicant shall be required to undergo shall be carried out vis-à-vis the other System Participants.
- 2.10.22. The Access Applicant shall deliver to the System Operator the book of tests it performed according to the directives delivered thereto by the System Operator.
- 2.10.23. The System tests shall be carried out in such timeslot as the System Operator shall allocate to the Access Applicant.
- 2.10.24. Tests shall also be carried out vis-à-vis other System Participants to confirm proper end-to-end activity.
- 2.10.25. In any case of test failure or continuation beyond the allocated timeslot, the Access Applicant may submit a written application for an additional timeslot for completion of the developments and adjustments required for activity in the Payment System.
- 2.10.26. It is clarified that in the context of the Access Applicant's logon to the accounting interface, "end-to-end" tests shall be carried out between the Access Applicant and the other System Participants. However, for the avoidance of doubt, the System Operator may connect the Access Applicant to the System also without completion

of the said tests, where the Access Applicant shall have completed all of the basic tests required by the System Operator.

#### 2.11. Go-live date according to "access windows"

- 2.11.1. The Access Applicant shall coordinate the go-live date with the System Operator according to the technological resources required from the perspective of the System Operator and the "access windows" determined thereby, and according to the Access Applicant's readiness, as shall be determined by the System Operator, the Oversight of Payment Systems at the Bank of Israel and the regulator of the Access Applicant.
- 2.11.2. The connection to the System will be possible in "access windows" on two dates a year, in the months of **January** and **July**. The "access window" dates may change, as shall be determined by the System Operator and subject to the number of Participants approved to logon in each "access window" (up to 3 Participants), all according to the System Operator's discretion.
- 2.11.3. In any case where the Participant shall have chosen to be a RTGS System Direct Participant – the Payment System Access Window is contingent on completion of the connection to the RTGS System. The Participant is responsible for taking action to synchronize the go-live of the Charge Card system with the RTGS System.
- 2.11.4. According to the selected timeslot, the System Operator shall inform the other System Participants of the Access Applicant's go-live date, and of new participant onboarding plan, which includes the tests that are required to be performed for its entering the System.
- 2.11.5. In the event that the Access Applicant completed most of the necessary developments and/or adjustments, and has a number of minor adjustments remaining, in proximity to the Access Window time, at the discretion of the System Operator – the System Operator shall allow, by prior arrangement, a postponement by another month for the completion of all required processes and going live a month later than the predefined Access Window.
- 2.11.6. **In the event that the Access Applicant fails to complete the necessary adjustments during the additional period, it will be required to coordinate a new date in accordance with the determined "Access Windows" as aforesaid, including readiness in terms of development, tests and renewed authorizations.**

#### 2.12. Granting of confirmation of completion of logon process

- 2.12.1. After the successful completion of the connection tests, the System Operator shall send confirmation to the Oversight of Payment Systems at the Bank of Israel for the successful completion of all technological and legal aspects required for commencement of activity in the System.

#### 2.13. Receipt of authorization to go live

- 2.13.1. The Access Applicant shall become a System Participant and be entitled to operate in the System only after completing the full login process to the System, as detailed above and below, and only after the System Operator has received the authorization of the Oversight of Payment Systems at the Bank of Israel to go live to start its activity as a System Participant.

- 2.13.2. The Oversight of Payment Systems at the Bank of Israel shall inform the System Operator regarding authorization of the Access Applicant to operate in the production environment.
- 2.13.3. The System Operator shall notify all of the System Participants, in accordance with the access window established above, on the start of activity of the new System Participant. Such notice shall include details on the new Participant, including – name, address and the official date of commencement of its activity in the System.
- 2.13.4. The Access Applicant shall operate in the Payment System in the production environment.

#### **2.14. Pilot in production**

- 2.14.1. After the System Operator has received authorization of the Oversight of Payment Systems at the Bank of Israel, for the activity of the new Participant in the Payment System in the production environment, the Participant shall operate in the production environment in a gradual and reduced manner under the conditions and for a period that shall be coordinated between the System Operator and the new Participant, and at the discretion of the System Operator and its instructions.

#### **2.15. Logon of CLP Operators to the Payment System**

- 2.15.1. Before logon to the System, the CLP Operator shall be required to sign an agreement with the System Operator, that is adapted to the requested activity, which shall include the technological connection requirements that it shall be required to meet.
- 2.15.2. The CLP Operator is required to receive confirmation from the National Cyber Directorate on meeting the YUVAL methodology, and present a valid confirmation upon demand.

### **3. The System's Services**

#### **3.1. General**

- 3.1.1. The services provided by the System Operator are with respect to charge card brands that are cleared in Israel by the System Participants, as defined in these Rules.
- 3.1.2. Adding additional charge card brands to the approvals and collection interface shall be done in advance and in writing between the Acquirer and the System Operator.

#### **3.2. Description of the System's environment**

The System environment includes several key components with the System Operator and the Participant that is connected to the Participant with Direct Technical Connection:

##### **3.2.1. System components with the System Operator**

- 1) A computer system that handles online communication with the Businesses and with the Participants.
- 2) A computer system that handles the processing of the transactions and their distribution to the Acquirers.

- 3) A computer system that handles the accounting process between Issuers and Acquirers.
- 4) A secure file transfer system.

### 3.2.2. System components with the Participant with Direct Technical Connection

- 1) A computer system that handles online communication with the System Operator.
- 2) A computer system that handles the processing of the transactions received from the System Operator and transferring them to the accounting interface.
- 3) A secure file transfer system.

## 3.3. Technical aspects

### 3.3.1. Physical logon of a Participant

- 1) Logon to the System shall be performed via TCPIP communication on dedicated communication lines – one line for the main site of Shva in Holon, and a second line for the secondary site in MED1.
- 2) In the event of a line failure, it is required to immediately switch automatically without manual intervention, to the additional line available at the secondary site. Shva provides the connectivity between the two sites for a transparent transition.
- 3) Line inspection – Twice a year, a line inspection is required, in collaboration with the Shva team, by moving to the secondary line and working for a minimum of one hour.
- 4) It is the Participant's responsibility to ensure, through its internal systems, immediate recovery (without manual intervention) of the applicative/communication application after the line goes down and comes back.

### 3.3.2. Delivery and receipt of files to and from the Participant

The Participant is required to use safe room technology for the secure file transfer.

### 3.3.3. Delivery of information/reports to and from the Participant

The delivery shall be made via e-mail, a secure safe in accordance with the classification of the transferred information, and in accordance with the decision of the System Operator at its sole discretion.

## 3.4. Services for the Acquirer

- 3.4.1. Every day, various data files are transferred to the Acquirer for continued handling, monitoring and control of their activity in the Payment System; The transfer of the information shall be made using a secure file transfer system.

#### Daily transactions file

Every day after the daily transaction processing, the System Operator sends to each Acquirer the file of the daily transactions that it cleared, including the calculation of the appropriate benefit pursuant to the loyalty program interface rules.

<b>Raw transactions file</b>	At the Acquirer's request, the System Operator shall act to transfer the Acquirer the transactions transferred from the terminals in its Clearing during the day, in their raw configuration.
<b>Retailers file</b>	The transfer of the file to the Acquirer shall be done after the completion of daily retail processing each Business Day.
<b>Accounting information file</b>	The accounting processes are carried out after the daily processing of the transactions. During the processing, the information is concentrated for the purpose of producing the charges for the System Participant (for the services provided thereto) and a file is produced that is intended to assist the Participant in checking the daily charge.

- 3.4.2. **Advice** – An FYI message containing the approval request data to be sent to the Issuer or Acquirer in the event that an approval request message is not sent for their approval. The message will be sent to such party in order to inform about the approval request.
- 3.4.3. **Connection and management of Terminals** – as specified in Section 4 to these Rules.
- 3.4.4. **"End-of-Day Communication" – Updating parameters in the Terminal.** Upon the performance of "end of day" communication of a Terminal, the following actions are performed:
- 1) Transfer of update of the parameter values determined by the Acquirer for the Cleared Brands relevant to the Business, after processing retailers, if the values of the parameters have changed, as described in the EMV Protocol.
  - 2) Transfer of the values of the general vectors that refer to the Acquirer in Businesses in its Clearing. The list of vectors as described in the EMV Protocol.
  - 3) Receipt of the Transactions from the Terminals at the Businesses and their transfer to the daily processing system (prior to the transfer to the Acquirer) and provision of evidence to the Terminal, which confirms receipt of such data.
  - 4) Transfer of the Blocked Cards File to the Terminals.
  - 5) Transfer of parameters to Pin-Pad.

### 3.5. Services to the Issuer

- 3.5.1. Loading the values of the vectors as received from the Issuer, to all of the updated Terminals in the System.
- 3.5.2. Processing Transaction Approval Requests (for online verification):
- 1) Receipt of the Issue's response to the Transaction Approval Requests messages from the Terminals and their transfer to a Terminal.
  - 2) Stand in service – in accordance with unique rules established by each of the Issuers as delivered to the System Operator, provision of a response by the System Operator on behalf of the Issuer to the request for approval of Charge Card transactions, in cases where the Issuer is not available, or in cases that will be agreed in advance with the Issuer.



- 3) Transfer of online advice messages to the Issuers for responses to Approval Requests that were replied to by the System on their behalf.

### 3.5.3. Full Blocked Cards File

- 1) Receipt of the Issuer's Charge Cards file, that are not entitled to make Transactions at the Terminal.
- 2) The Blocked Cards File, including the degree of the block and the method of handling, shall be delivered by the Issuer to the Company by 14:00 on a Regular Business Day and by 12:30 on a Short Business Day.
- 3) Daily Blocked Cards processing, which is carried out after receipt of the Blocked Cards File from the Participants and no later than 15:00 on Regular Business Days and 13:00 on Short Business Days. In cases where any of the System Participants have not transferred a Blocked Cards File by the time stated above, the System Operator will carry out the processing based on the latest Blocked Cards File received from the Participant.
- 4) Building a full Blocked Cards File according to the capacity of the various types of Terminals and their transfer to the Terminals.
- 5) The space assigned to each System Participant in the Blocked Cards File is relative to the number of active cards of each one.
- 6) This service is carried out once on a Regular and Short Business Day, as part of the processing of the blocked cards. Each working day, a new generation of Blocked Cards File is built, which is created by Shva by merging and sorting all of the Blocked Cards Files received from the Issuers and the Acquirers, and cancellations and additions from the previous file are transmitted to the Terminals.
- 7) A full transmission of a Blocked Cards File is made upon:
  - (a) The establishment of a new Terminal.
  - (b) The generation gap between the Terminal and the central computer is greater than as defined by the System Operator.
  - (c) The Blocked Cards File in the Terminal is corrupted.

### 3.5.4. Small Blocked Cards File

- 1) Receipt of online Advice messages which include the numbers of the blocked cards for delivery to the Terminals ("**Small Blocked Cards File**").
- 2) The System creates a file containing 100 blocked cards out of the cards that were updated in the full Blocked Cards File during the day (on-line update).
- 3) The file is updated several times an hour, and a time stamp is inserted on each update, which states the time of update.
- 4) The file is fully transmitted and replaces the file that preceded it during Terminal communication.
- 5) The transfer of the Small Blocked Cards File to the Terminal is done during the timeslot of the System waiting for the Participant's response – but no more than once an hour.



### 3.6. Services to the CLP Operator

- 3.6.1. Infrastructure enabling the honoring of consumer loyalty program cards (Closed Loop Payments) as part of the Charge-Card Payment System.
- 3.6.2. In CLP activity, the operating party acts both on the issuing side and on the Clearing side.
- 3.6.3. Loading the vector values as received from the CLP Operator.
- 3.6.4. Processing Approval Requests (for online verification) vis-à-vis the CLP Operator, receiving a response to Transaction Approval Requests messages, and transferring them to the Terminal.
- 3.6.5. Connecting and maintaining Terminals.

### 3.7. Additional services

- 3.7.1. In addition to the basic services specified in Sections 5 through 8 as detailed below (the "**Basic Services**"), and subject to the approval of the System Operator, the System Participant shall be entitled to receive from Shva also specific technological developments that are over and above the services specified in these Rules (the "**Additional Services**").
- 3.7.2. A System Participant may ask Shva to perform Additional Services therefor, that are not included in the Basic Services provided by the System. It is clarified that the development of the Additional Services and/or the provision of the Additional Services are at Shva's sole discretion.
- 3.7.3. The System Participant is aware that if the System Participant submits the request for Additional Services before the System Participant has completed the process of logging on to the System for receipt of the Basic Services, this may extend the amount of time required for Shva to provide the Basic Services.
- 3.7.4. Ordering the Additional Services shall be carried out according to the following stages:
  - 1) The System Participant shall submit a request to Shva that shall include a list of the Additional Services it requests that Shva develop thereto, over and above the Basic Services that Shva provides through the System. The System Participant shall attach a specification of requirements at a high level of detail, and supporting documents that shall enable Shva to assess the degree of investment required by Shva to provide the Additional Services.
  - 2) If necessary, Shva shall hold several meetings with the System Participant to clarify the needs with a view to examine the request for the Additional Services, and whether the requested needs may be met within the framework of the existing Basic Services.
  - 3) Shva shall review feasibility and assessment of the degree of investment required in order to provide the Additional Services requested as part of the request, and shall prepare a price quote for the execution of the work.
  - 4) After the System Participant signs the price quote, based on the final calculation (subject to the order of priorities of the System Operator), Shva's Additional Services development project shall begin and, to the extent necessary, if developments and adjustments are also required by the Participant, the Participant shall start performing

the same. It is clarified that the development shall be carried out subject to the System Participant's approval of the characterization documents transferred from Shva.

- 5) Shva shall prepare and deliver to the System Participant a test specification for the new developments, that shall also include the tests to be performed vis-à-vis the System Participant. Shva shall perform the required tests for the new developments, according to the above test specifications.
- 6) To the extent necessary, the System Participant shall also carry out developments and adjustments in its systems, at its expense and responsibility, so as to make use of the Additional Services requested thereby.
- 7) The System Participant shall carry out thorough tests on its premises before seeking to carry out tests vis-à-vis Shva. At the end of the tests, the System Participant will send Shva the tests specification given thereto by Shva, signed and filled out thereby, and a statement signed thereby to the effect that it has successfully completed all of the tests required for receipt of the Additional Services from Shva, and that it requests that Shva perform the required tests on its behalf before receipt of the Additional Services.
- 8) The System Participant shall notify Shva of its readiness to perform the tests. The tests shall be carried out in a time window that Shva will assign to the System Participant. In the event of a failure in the tests, or if the tests continue over and above the allotted timeslot, the System Participant may request an additional timeslot. The timeslot shall be allocated according to Shva's ability.
- 9) If necessary, it is possible that some of the tests that the System Participant will be required to take will be carried out with each one of the System Participants, and the Participant will deliver to Shva a confirmation from each System Participant about the success of the tests therewith.
- 10) Upon completion of the tests, the System Participant will be able to receive the Additional Services, provided that it has completed the System logon process, and that Shva will coordinate with the System Participant the date of receipt thereof.
- 11) After completion of the development and the transfer to production, the Additional Services will be added to all of the services that the System Participant receives from Shva through the System.

### 3.7.5. Costs for the Additional Services

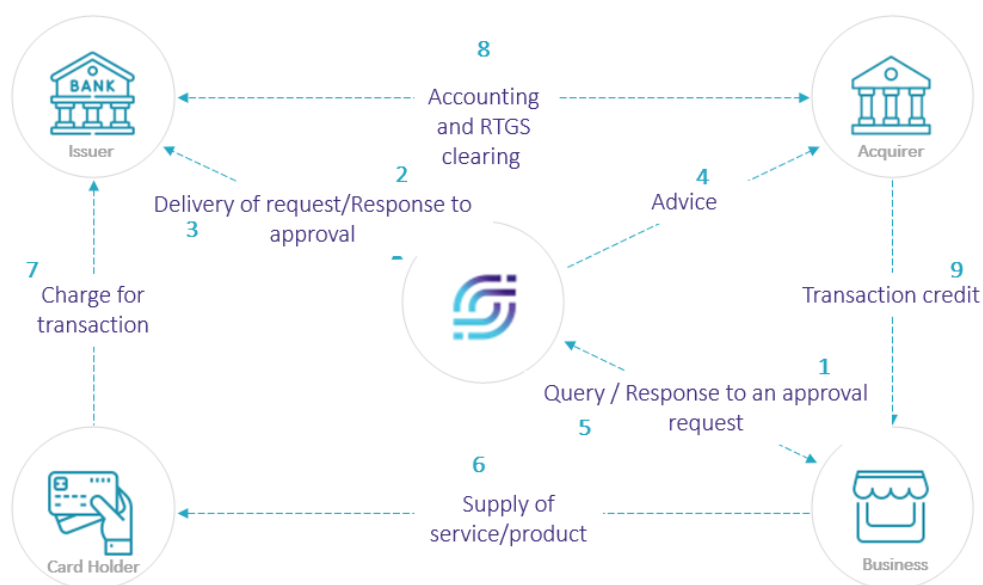
- 3.7.5.1. The costs for the Additional Services will be calculated on the basis of the designated pricing that will be determined for the Additional Services ("**Costs for the Additional Services**") which shall be paid by the System Participant in accordance with Shva's standard payment terms, where the method of payment shall be determined at the sole discretion of the Company. The payment shall be made against a lawfully prepared tax invoice. Such invoice shall include Shva's standard payment terms.
- 3.7.5.2. Shva shall be entitled to update from time to time, the hourly rates as specified above, as updated in the pricing schedule posted on the Company's website.
- 3.7.6. Where the System Participant chooses to receive Additional Services that are not defined in these Rules, as aforesaid, the Additional Services will be added to these Rules or, the System Participant will be requested to sign a dedicated agreement for such services, at the Company's discretion. Sections of intellectual property (17),

liability and indemnification (2.3, 14.1, 18) and ownership (1.8) that appear in these Rules shall also apply to the Additional Services.

### 3.8. Management of a central database

3.8.1. Management of a central database for displaying information regarding the management of the Terminal, and regarding Transactions carried out at the Terminals, in accordance with the provisions of the law.

### 3.9. Description of transaction process in Charge Card



## 4. Connection and Managment of Terminals

### 4.1. General

- 4.1.1. Requests to connect Terminals to the Charge-Card System may be received from the EMV software manufacturer and/or a software distributor that engaged in an agreement with the EMV Software Manufacturer.
- 4.1.2. It is possible to logon to the System only via Terminal models that the System Operator tested, authorized and approved for operation, and in accordance with the EMV Standard required in Israel.
- 4.1.3. The approved list of Terminals is displayed on the Company's website.

### 4.2. Functionality

4.2.1. Below is a description of the current functionality in the System:

- 1) Opening/closing/removal of a brand at the Terminal.
- 2) Update of Caps, Parameters and vectors to the Terminal.

- 3) Management of Blocked Cards File and their update on the Terminal.
- 4) Management of Clearing transitions – replacement of Acquirer for the Business.
- 5) Information transfer service.

#### **4.3. Opening a Terminal**

- 4.3.1. Receipt of requests to open a Terminal, and entries thereof in the Retailers System.
  - 1) Reception of the requests shall be automated.
  - 2) Automated requests that shall reach the Company by 15:00 on a Regular Business Day or by 12:00 on a Short Business Day, shall be processed on that Business Day.

#### **4.4. Requests for approval of a Clearing Brand**

- 4.4.1. The transfer of a file of requests for approval of a brand to the relevant Acquirer in the Terminal:
  - 1) The file shall contain the details of the Terminals whose opening requests were received from the software distributors or EMV software manufacturers, and were received in the Retailers System on the same Business Day.
  - 2) This service is performed twice a day, in an automated manner:
    - 1.1) Commencement of Business Day, to be sent by around 11:00.
    - 1.2) At the end of a Regular Business Day, after 16:30 and by 17:30 at the latest, and on a Short Business Day, after 15:00 and by 15:30 at the latest.

#### **4.5. The opening of brands and update of Parameters**

- 4.5.1. Receipt of a file from the Acquirer, which includes:
  - 1) Approval of requests for approvals to clear a Cleared Brand in the Business, and determination of Parameters, Authorizations and Caps with respect to the approved Cleared Brand.
  - 2) Update of Parameters, Authorizations and Caps with respect to Cleared Brands at other Businesses.
- 4.5.2. Receipt of the file shall be permitted up to 3 times on a Business day (Regular and Short) and no later than 16:00 on a Regular Business Day or 12:00 on a Short Business Day.

#### **4.6. Closure of Brands/Closure of Terminal for Activity**

- 4.6.1. An Acquirer-type System Participant may, at its sole discretion, inform the System Operator that a certain Business may not be allowed to continue using the System's Approval and Collection Interface regarding its activities therewith.
- 4.6.2. An Acquirer-type System Participant that notified the System Operator as aforesaid, shall be responsible for continued handling vis-à-vis the Business. It is clarified that Shva is not a party to the issue, and that it operates in accordance with the instructions of the Acquirer System Participant only.

- 4.6.3. Receipt of a messages file from the Acquirer to stop Clearing a Cleared Brand in a Business, will be possible several times during a (Regular and Short) Business Day, and no later than 15:00 on a Regular Business Day or 12:00 on a Short Business Day.
- 4.6.4. If the System Operator has received such notification, the System Operator will flag the aforesaid Business as a "blocked" Business, which will mean that after the daily processing of the Retailers, any approval request received from such Business, regarding any specific transaction, will not be approved, and that after the transfer of a file of transactions from the Terminals of such Business to the Company for processing and transferring them to the System Participant who requested the blocking, the Business will be blocked with the relevant brand vis-à-vis the Acquirer, such that future transactions (over and above the transactions that have passed in the said Transactions file) will be blocked.
- 4.6.5. The System Operator may also block a Terminal from activity where the System Operator detects abnormal operation of the Terminal and there is concern of fraud and/or information security problems and/or any other action that may endanger the System. Notice of the blocking will be given in writing to the relevant Acquirers at the Terminal.
- 4.6.6. Blocking due to inactivity in a multi system – in cases where a Terminal has not been active and did not transmit Transactions for 3 months, it will be blocked due to "inactivity". The Business may (through the entity that opened the Terminal therefor) request to unblock the Terminal within 3 months from the date of the block. Unblocking a Terminal also requires the approval of the Acquirer to reopen it. After another 3 months the Terminal shall be removed from the System.

#### **4.7. Clearing endorsement**

- 4.7.1. Receipt of a messages file of a System Participant to start Clearing a Cleared Brand at the Terminal that was cleared by another Participant (endorsements).
- 4.7.2. Receipt of the file shall be possible up to twice on a Business Day (Regular and Short) and no later than 15:00 on a Regular Business Day or 12:00 on a Short Business Day.
- 4.7.3. The System Participant shall coordinate with the System Operator, inasmuch as possible, the time at which it wishes to transfer the files.
- 4.7.4. Such endorsement shall be carried out as part of the Retailer processing (as specified below) which will be carried out on the following (Regular and Short) Business Day and apply to Transaction transmissions received in the System after midnight on the aforesaid Business Day.

#### **4.8. Daily retailer processing**

A daily retailer processing is carried out each Business Day (Regular and Short), after completion of receipt of the files for opening Terminals from the Participant, and no later than 17:00 on Regular Business Days and 13:00 on Short Business Days.

## 5. Approvals Interface

### 5.1. General

- 5.1.1. The System receives and processes approval requests from Terminals 24/7, all year round, subject to its availability.

### 5.2. Functionality

- 5.2.1. Below is a description of the current functionality at the **online approvals** interface:

- 1) Receipt of Transaction Approval Requests from the Terminals, their routing to the System Participants and returning a response to the Terminal.
- 2) Sending Advice messages to the opposing Participant (to the Acquirer or Issuer to which the Approval Request was addressed in the previous section)
- 3) Response to approval requests on behalf of the System Participant (Issuer) in accordance with the limitations and authorizations received from such Participant (stand-in mode).

### 5.3. Days and hours of activity

- 5.3.1. The System receives and processes approval requests (Approval Interface) and collection of transactions from the Terminals 24/7 all year round, subject to its availability.
- 5.3.2. The effective date for an approval request is as recorded in the Terminal.

### 5.4. Description of interface activity

- 5.4.1.1. Each Transaction Approval Request is checked by the System locally, vis-à-vis the Terminal software:
- 1) **Blocked cards check** – checking that the Charge Card is not in the Blocked Cards File in the Terminal and in the Small Blocked Cards File. In the event that the Card is in the (large or small) Blocked Cards File, the System returns a negative answer to the Business, "card blocked or stolen" (depending on the reason for the block in the file) and prevents the transaction from being carried out. If the above query ("Blocked Cards check") passes the check, the System continues to perform a "Usage Check".
  - 2) **Usage check** – checking whether the transaction amount is higher than the permitted cap (for the card or the Business). In the usage check, the System ensures, vis-à-vis the Usage File, whether the Charge Card carried out transactions that meet the criteria defined by the Issuer regarding the cumulative amount of the transactions and the cumulative number of transactions. If the card does not meet the criteria, the System returns a negative answer "call the credit company". If the card meets the criteria, the System performs additional logical checks.
  - 3) **Additional logic checks** – The System continues and performs additional checks, in accordance with the Rules defined by each Acquirer-type or Issuer-type System Participant. These checks and Rules are not uniform among the Participants and depend on the requirements of each Participant.

5.4.1.2. In accordance with the results of the additional logic checks, the transaction request is finally approved, finally rejected, or the following clause applies: "transmission for approval".

#### 5.4.2. "Transmission for approval"

5.4.2.1. A Transaction Approval Request goes from the Terminal through the communication network to the System in real time. The System Operator performs tests for the approval request in accordance with the guidelines defined by each Acquirer-type or Issuer-type System Participant or both. A request that fails the threshold tests is accompanied by a negative response to the Transaction Approval Request without forwarding it to the System Participant. A Transaction Approval Request that has passed the test is forwarded through the Branding System for the approval of the System Participant:

- 1) **Local transactions** – transferred to the Issuer, on behalf of the Acquirer. The Issuer returns a response (approval or rejection of the transaction) through the Branding System and after a (technical) compatibility check between the query sent to the Issuer and the response received from the Issuer, the response is forwarded to the Business. Information about the transaction, including the Issuer's response, is also transferred to the Acquirer as an advice message sent at the end of the process.
- 2) **Tourist transactions** – transferred to the Acquirer. The Acquirer returns a response (approval or rejection of the transaction) through the Branding System and after checking the compatibility between the query sent to the Acquirer and the response received from the Acquirer, the response is forwarded to the Business.

#### 5.4.3. Stand In Process

5.4.3.1. Stand In Process is a process in which tests are performed by the System in accordance with agreed rules defined in writing by each of the System Participants, in order to deliver a response to the Business, instead of the System Participant.

- 1) The System waits for the response of the System Participant within a predetermined time which may change from time to time according to the System's needs, and in coordination with the System Participants. When the time expires, the System responds according to the rules established for each System Participant.
- 2) Where the System is in a state of Stand In Process service, and the approval system will respond to the Business instead of the System Participant. After that, an advice message will be sent to the Acquirer and the Issuer.

### 5.5. Point of No Return and Payment Instruction Finality

5.5.1. **Point of No Return** in the Approvals Interface is a point of time in which the response of the Participant is transferred and orderly received by the Terminal.

5.5.2. **Payment Instruction Finality Date** in the Approvals Interface is the date in which the approval is recorded as a transaction in the Terminal.

### 5.6. Possible Failure Scenarios

The scenarios described in the table below describe possible failures both on the part of the System Operator and on the part of the System Participants in the interface, and how the failure is handled:



#	Scenario	Method of handling
1	<b>Failure in means of communication</b>	The System Participants are responsible for the ongoing maintenance of the communication equipment under their responsibility, including the communication line between them and the System, even if the equipment is located in the premises of the System Operator. The System Operator will allow access to the System Participant for the maintenance of its equipment 24/7 by prior arrangement.
2	<b>On-line messages, approval requests</b>	In the case of failure of the System Participant in returning a response to the transaction request, the System Operator may provide stand-in services as specified in Section 5.4.3 of the Rules.
3	<b>Failure event of the System Operator</b>	In the case of a failure event with the System Operator, the System Operator shall take the relevant steps to resolve the event as described in Section 12.3 of the Rules in order to continue adequate operation of the System. Insofar as the failure event affects and is relevant to the activity of the System Participants, the System Operator will notify the contacts of the System Participants within a reasonable period of time under the circumstances, of the failure event and its consequences.

It is clarified that the System Operator shall not bear any direct and/or indirect damage to be caused, if caused, to the System Participants and to any third party as a result of malfunctions or delays as aforesaid.

## 6. Transaction Collection and Processing Interface

- 6.1.1. The System handles and processes the transactions collected from the Terminals in the timeslot that had passed since the processing that preceded it.
- 6.1.2. The process of intake of the transactions, sorting them and dividing them into Acquirers is done taking into account and implementing the Rules and instructions received from the Acquirers and Issuers regarding discounting companies and customer loyalty programs. When finished, the files are transferred to the Acquirers through safes.

### 6.2. Functionality

- 6.2.1. Below is a description of the current functionality in the interface:
  - 1) Receiving raw transaction file transmissions from the Terminals and transferring them for processing.
  - 2) Processing daily entries and generating daily transaction files for the relevant Acquirers in the Terminals.



### 6.3. Activity days and times

- 6.3.1. The System handles and processes the transactions collected in batch processing processes on Business Days.
- 6.3.2. Ordinary daily transaction processing takes place every (Regular and Short) Business Day as specified in Section 6.4.2 of the Rules.
- 6.3.3. Additional transaction processing is carried out on several days a month as specified in Section 6.4.3 of the Rules.
- 6.3.4. The System Operator may make changes to the days and hours of activity of the System subject to the provisions of Section 1.9 of the Rules.
- 6.3.5. The System Operator shall notify the System Participants in writing of the change in the days and hours of activity and the planned date for implementing the change. In the event of a change in the operating hours that requires the System Participants to prepare, a notice of two weeks will be given in advance.
- 6.3.6. The effective date for the receipt of a Payment Instruction to the System is the time of entry of the Payment Instruction into the System, as recorded in the System Operator's computers.
- 6.3.7. All of the transactions that reached the System by the start time of normal processing (transaction cut-off time) will be associated with the Participants on the Business Day preceding the processing day.

Day of the week	Transaction cut-off time
Weekdays, Fridays, holiday weekdays and holiday eves	07:00
Saturday, holiday, bank holiday	No ordinary transaction cut-off

- 6.3.8. All of the transactions that reached the System until the start time of the additional processing, (transaction cut-off time), will be associated with the System Participants on the Business Day on which the processing was performed.

Day of the week	Transaction cut-off time – Additional processing
Weekdays, mid-Holidays, end of Shabbat and end of holiday	20:00
Friday, holiday eves	13:00

#### 6.3.9. A System Participant's request for time extension

- 1) In an exceptional case, a System Participant may contact the System Operator with a request to move forward or delay the times of daily processing, additional processing as defined in these Rules, or to perform additional processing on a specific day that is not defined in these Rules.
- 2) The System Operator shall consider each such request made thereto.
- 3) The System Operator may approve the System Participant's request if it believes that there is no concern of damage to the System's activity. If such extension is approved, it will be valid only for the day of service on which such request was submitted.

- 4) The System Operator shall inform all of the System Participants, as early as possible, about the making of such change.

#### 6.4. Description of Interface Activity

6.4.1. Transactions are collected during end-of-day communication from the Terminal to the System. The collection of transactions includes the following four stages:

- 1) **Identification of the Terminal with the System** – the identification process is as described in the EMV Protocol.
- 2) **Transmission of parameters, vectors and technical details** – parameters and vectors that are relevant to the Terminal and have undergone a change, are transmitted from the System to the Terminal together with technical details for synchronization purposes.
- 3) **Transmission of the transactions from the Terminal to the System** – at the end of the transmission of the transactions, a notification is received on the Terminal indicating the completion of the transmission. If the transmission was not completed successfully, the Terminal operator is required to initiate a retransmission of all transactions from the beginning.
- 4) **Transmission of Blocked Cards File in the Terminals, by the System**

#### 6.4.2. Daily transaction processing

- 1) Daily transaction processing takes place every (Regular and Short) Business Day. Transaction processing starts at 07:00 and ends (except in the case of an operational failure) no later than 11:00.
- 2) In cases where an unusually large transaction file is received (15% or more of the average daily number of transactions in the last month) and as a result the System Operator is unable to transfer the transaction files to the System Participants by the time specified above, the files will be transferred at the earliest possible time.
- 3) Transactions received (from the Terminals) before the start of processing will be included in the daily transaction processing and transferred to the System Participant after the daily transaction processing.

#### 6.4.3. Additional transaction processing

- 1) During the calendar month, additional processing is carried out, that includes transactions transmitted to the System by 20:00 on a Regular Business Day, Saturday evening and holiday evening or by 13:00 on a Short Business Day.
- 2) Transactions from such processing will be transferred to the Acquirers participating in the System, by 22:00 on the same day on a Regular Business Day, on Saturday evenings and holiday evenings or by 15:00 on a Short Business Day.
- 3) The additional processing is made on the dates below:

The additional processing days in a calendar month	If the additional processing day falls on a Regular Business Day	If the additional processing day falls on a Short Business Day	If the additional processing day falls on a Bank Holiday
1	The additional processing is	The additional processing is	The additional processing is

	performed on the 1st of the month	performed on the 1st of the month	performed on the 1st of the month
9	The additional processing is performed on the 9th of the month	The additional processing is performed on the 10th of the month	No additional processing
14	The additional processing is performed on the 14th of the month	The additional processing is performed on the 14th of the month	No additional processing
15	The additional processing is performed on the 15th of the month	The additional processing is performed on the 15th of the month	The additional processing is performed on the 14th of the month
19	The additional processing is performed on the 19th of the month	The additional processing is performed on the 20th of the month	No additional processing
25-31	The additional processing is performed between the 25 <sup>th</sup> and 31 <sup>st</sup> of the month	The additional processing is performed between the 25 <sup>th</sup> and 31 <sup>st</sup> of the month	No additional processing

- 4) A System Participant may request additional dates from the System Operator in order to carry out additional processing as aforesaid. The System Operator shall consider any such request that is presented thereto and decide whether to respond to the request according to the following criteria in the context of the System:
- The criticality of the date (the scope of activity in terms of quantity and sums of money).
  - The stability and activity of the System (treatments, the state of the computer and communication center, running times, failure events).
  - The frequency of the special processing.
  - Other limitations and requests.
  - Impact on other System Participants.
  - The meaning and consequences of non-fulfillment of the request.
  - If a date for additional processing is added as stated, such date will be updated in the System Rules and additional processing will be performed as stated with respect to all System Participants.
- 5) Each System Participant is required to receive the file created from the additional processing and integrate it into its own processing.
- 6) The System stores the transaction data made at the Terminals and transferred thereto for a period of 7 years from the date of receipt thereof.

## 6.5. Point of No Return and Finality of Payment Instruction

- 6.5.1. **Point of No Return** – in the collection interface is a point of time in which the Terminal ended the transmission of the transactions and these are orderly received by the System Operator.
- 6.5.2. **Payment Instruction Finality Date** – in the collection interface and the processing of transactions is the date on which the "Daily Transactions Processing" file is transferred to the Acquirer.

## 6.6. Possible failure scenarios

The scenarios described in the table below specify possible failures both on the part of the System Operator and on the part of the System Participants in the interface, and how the failure is handled:

#	Scenario	Method of handling
1	<b>Transaction collection</b>	In the event of a technical failure in the collection of transactions from a certain Terminal, the Terminal operator may repeat the act of transmitting the data to the System Operator. If necessary, it is required to find out the reasons for the failure with its system provider.
2	<b>Failure in the transfer of transaction files</b>	In cases where the System Operator is unable to transmit the transaction files to the System Participants by the specified time according to Section 6.3, the files will be transmitted at the earliest possible time. System Participants are required to maintain a mechanism to consolidate multiple transaction files sent by the System Operator in their processing / or to receive all of the files.
3	<b>Inadequate information</b>	Inadequate information that reaches the System shall be rejected and not processed by the System.
4	<b>Failure event of the System Operator</b>	In the case of a failure event of the System Operator, the System Operator will take the relevant steps to resolve the issue as described in Section 12.3 in order to continue adequate operation of the System. If the failure event affects and is relevant to the operations of the System Participants, the System Operator will notify, within a reasonable time under the circumstances, the Participants' contacts about the failure and its consequences

It is clarified that the System Operator shall not bear direct or indirect damage to be caused, if any, to the Participants and any third party, as a result of malfunctions or delays as aforesaid.

## 7. Accounting Interface

### 7.1 General

- 7.1.1. Every Business Day, each Acquiring-type Participant who is a System Participant, sends a file to the System, containing a list of cross transactions in which it is the Acquirer

and not the Issuer, for which it requests to continue processing with the relevant Issuers in order to collect payment for the transactions.

- 7.1.2. The interface handles the accounting processes between the Acquirers and the Issuers in the Charge-Card Payment System.

## **7.2. Functionality**

- 7.2.1. Below are the services provided by the System Operator to the System Participants, through the System:

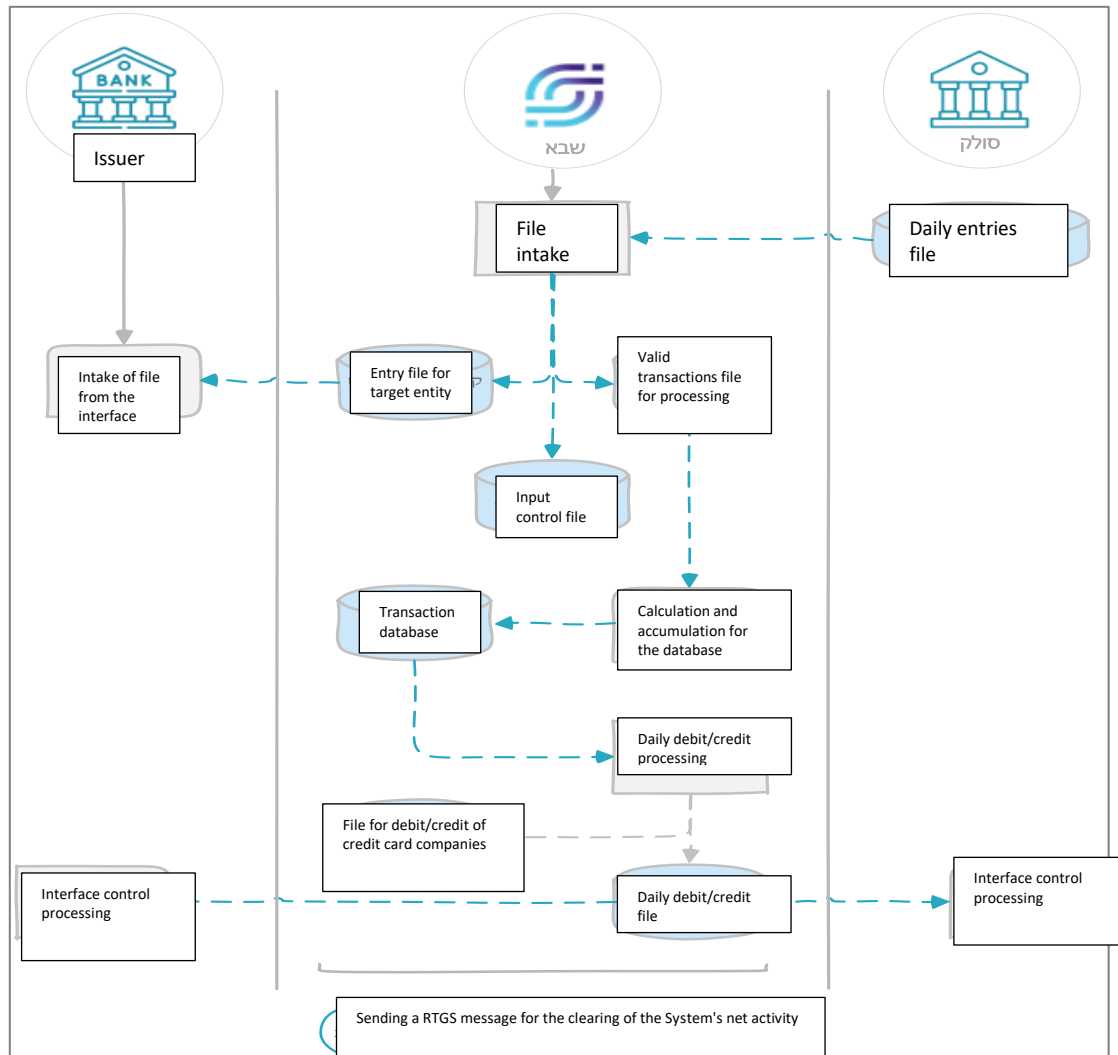
- 1) Intake, sorting, and splitting of transactions according to the System's specification documents for the supported brands.
- 2) Accounting and transfer of funds and information between Acquirers and Issuers for transactions/entries where the Acquirer and Issuer are different Participants.
- 3) Preparation of files for System Participants and transferring them to the System Participants.
- 4) Calculation of the Net Values between System Participants and sending the Net Results to the RTGS for Settlement between the System Participants.

## **7.3. Description of the System environment**

- 7.3.1. The System environment includes 7 main components at the System Operator and the System Participant:

- 1) Safes used for the secure transfer of files between the System participants and vice versa.
- 2) Transaction databases for each Acquirer – a database that contains all of the Acquirer's transactions for the last 7 months and/or 2 years if special activity has been performed on the transaction.
- 3) Input file – an entries file in which the System Participant debits/credits the target party (the Acquirer or the Issuer).
- 4) Financial entries file – transferred to the target party and contains entries that have been received by the System on a daily basis.
- 5) Credit/Debit file – transferred to the System Participant and the target party, containing the accounting entries.
- 6) Net settlement file – the file from which the message for the Settlement of the Net Values will be derived.
- 7) Future balances file – transferred to the System Participant on a monthly basis and contains all future transactions of the System Participant.

7.3.2. The flow of information in the System is illustrated in the diagram below:



#### 7.4. Days and hours of processing in the interface

##### 7.4.1. Timing of the processing cycle in the accounting interface

File name	Days	Time of sending files to Shva/files leaving Shva	In exceptional cases and with the approval of the System Operator
Incoming entry file from the Acquirers	Sundays to Thursdays and Mid-Holidays	15:00	16:00
	Fridays and holiday eve	13:00	14:00
	Saturday, Bank Holidays and holidays	--	--

<b>Outgoing entry file to the Issuers</b>	Sundays to Thursdays and Mid-Holidays	19:00	--
	Fridays and holiday eve	17:00	--
	Saturday, Bank Holidays and holidays	--	--
<b>Credit/Debit file</b>	Sundays to Thursdays and Mid-Holidays	24:00	--
	Fridays and holiday eve	24:00	--
	Saturday, Bank Holidays and holidays	--	--

- 7.4.2. Accounting interface processes are performed only on Business Days (short or long).
- 7.4.3. If the 2nd day of the month falls on a Sunday or on a day following a holiday, except for the day after Yom Kippur, then the System Participants are allowed to send transaction files also on a Saturday or holiday. In this case, the files are required to reach the System by 16:00. At 16:00, or after all files have been received from the System Participants, whichever is earlier, the accounting interface processing will automatically begin. The automatic processing will send the outgoing transaction files to the System Participants by 19:00 and the credit/debit files by 24:00.
- 7.4.4. A System Participant may request a change in these times from the System Operator. The System Operator shall consider each such request that is presented thereto and shall decide whether to approve the request based on the following criteria:
- 1) The state of the System.
  - 2) The criticality of the date (scope of activity in terms of volume and amounts of money).
  - 3) System stability and activity (maintenance, data and communication center status, running times, failure events).
  - 4) Other limitations and requests.
  - 5) Impact on other Participants.
  - 6) The meaning and implications of non-fulfillment of a request.
- 7.4.5. The System Operator may, at its sole discretion, change the schedule outlined above with at least two weeks' notice to all System Participants prior to the change.

#### 7.5. System services in the accounting interface

- 7.5.1. Receiving transaction/entry files from System Participants: Receiving transaction/entry files from the Acquirer and the Issuer, and performing validity checks on the transactions/entries included in the file according to the "Validity Check" document (which includes details of logical validity checks on the input file).
- 7.5.2. Generating an input control file: The transaction/entry input file (input control file) containing the rejected entries is sent to the relevant System Participant who transmitted the file.

- 7.5.3. Generating a transaction/entry file: Generating an outgoing transaction/entry file for the relevant System Participant to whom the entries are intended, containing transactions/entries that were received (and not rejected) by the accounting interface.
- 7.5.4. Preparing System Participants' credit and debit files:
  - 1) Credit and debit of System Participants are carried out simultaneously between multiple System Participants, according to different types of agreements resulting from different types of cards.
  - 2) The System Operator shall prepare the credit and debit files for each System Participant according to predefined and agreed-upon Rules that were sent thereto in writing.
  - 3) These files include data on transactions performed at Businesses in Israel using charge cards issued thereby and by other Participants, with reference to and handling of:
    - 3.1) Interchange Fee.
    - 3.2) Payment transactions.
    - 3.3) Processing of Special Transactions.
    - 3.4) Calculation of conversions and linkages according to the exchange rates published daily by the Bank of Israel and the Consumer Price Index, as released monthly by the Central Bureau of Statistics.
- 7.5.5. Management of a database that shall serve for:
  - 1) Inquiry purposes, transaction identification, and the performance of special actions such as handling chargebacks, credit/debit of System Participants according to predefined and agreed-upon Rules by all System Participants, in accordance with all types of transactions/entries, and in this context, consideration of discounts, Interchange Fees, etc., as defined in the functional specification.
  - 2) Generating a detailed monthly balance file with respect to Base Transactions and Special Transactions.
- 7.5.6. Calculation of the Net Values between System Participants and sending the Net Results to the RTGS for Settlement between the System participants.
- 7.5.7. The System retains data of all transaction messages and additional messages received by the System, including information added thereto during processing, for inquiry purposes and data retrieval for 7 years from the date of their receipt in the System.
- 7.5.8. All of the files transmitted from the System to the System Participants are backed up for a period of 90 days.

#### 7.6. Description of the interface activity

- 7.6.1. **Start of day** – a Business Day is updated in the System at 11:00.
- 7.6.2. **Receipt of files** – receipt of files from all Participants and transmitting input control.
- 7.6.3. **Processing** – at 16:00, intermediate processing begins, and upon completion, financial entry files will be sent to all relevant Participants.
- 7.6.4. After updating the **foreign currency rates** as released by the Bank of Israel, the central processing process will begin, during which the databases and financial amounts will



be updated for the final calculation and production of credit/debit files that are sent to the Participants.

7.6.5. **End of day** – backups for all databases.

#### 7.7. Accounting rules in the interface

7.7.1. Accounting in the accounting interface is performed only in Shekel currency ("ILS").

7.7.2. The accounting between System Participants is independent and may differ from the accounting between the Acquirer and the Business, and between the Issuer and the Card Holder, in the following aspects:

- 1) **Dates** – The Business credit date, the Card Holder charge date, and the Issuer charge date and Acquirer credit date.
- 2) **Amounts** – The shekel amounts in which the Business will be credited, the Card Holder will be charged, and the amounts by which the interface will charge the Issuer and credit the Acquirer – for shekel transactions, dollar transactions, and CPI-linked and Dollar-linked transaction payments.

7.7.3. The Acquirer and the Issuer shall manage reconciliation mechanisms with the interface to ensure alignment between the data in the interface and the data held by the relevant Participants.

#### 7.8. Point of No Return and point of finality of the Clearing

7.8.1. **Point of No Return**

- 1) Is the point in time in which a Payment Instruction may no longer be canceled and/or modified by the System Participant.
- 2) Is defined as the time of commencement of processing of the files in the System, as specified in Section 7.6 of these Rules.

7.8.2. **Clearing finality date**

- 1) The Clearing finality date between the System Participants occurs with the completion of the final and absolute transfer of Payment Instructions between the RTGS Participants (completion of Settlement of Net Results) on the Business Day following the processing day.

#### 7.9. Possible failure scenarios in the accounting interface

The scenarios described in this table specify possible failures both on the part of the System Operator and on the part of the System Participants in the Accounting Interface, and the method of handling of a failure:

#	Scenario	Method of handling
1	<b>Communication failure</b>	In the event of a failure in the internal systems of the System Participants, which prevents them from working electronically with the System, the System Participants and the System Operator may take coordinated alternative measures, such as transferring the information through other means, in order to ensure receipt of the files by the accounting interface.
2	<b>Failure at Participant</b>	<ol style="list-style-type: none"> <li>1. A file that arrives at the System in an <b>incorrect format</b> will be rejected and not processed by the System.</li> <li>2. It is the sole responsibility of the System Participant to ensure that its files are in order, that there is no duplication between the files sent thereby to the Company before the failure occurred, and which have not yet been processed by the Company, and the files it sent to the System as part of the failure recovery process.</li> <li>3. Communication failures and any other failures occurring outside the System are not the responsibility of the System Operator. In such cases, the responsibility of the System Operator begins only once a correct file is received by the System's computers and which has passed the required checks.</li> </ol>
3	<b>Failure of the System Operator</b>	<ol style="list-style-type: none"> <li>1. In the event of a failure with the System Operator, the System Operator shall take appropriate alternative measures, such as transferring the information through other means, in order to receive or transmit the required information to the System Participants, and ensure the system continues to operate properly.</li> <li>2. The System Operator shall notify on the delay to the contacts of the relevant Participants.</li> </ol>

It is clarified that the System Operator shall not bear direct or indirect damage to be caused, if any, to the Participants and any third party, as a result of malfunctions or delays as aforesaid.

## 8. Clearing Interface – Clearing the System's Activity on the RTGS System

### 8.1. General

- 8.1.1. The system handles the Settlement processes of Net Activity between the Acquirers and Issuers in the Charge-Card Payment System.
- 8.1.2. The Settlement processes of Net Activity between the Acquirers and Issuers in the Charge-Card Payment System are carried out according to the RTGS Rules in Israel.
- 8.1.3. The System receives the accounting files as received from the System Participants and converts the file structure into a message format according to SWIFT requirements;

### 8.2. Settlement of the System's Net Activity

- 8.2.1. The System Operator provides System Participants with Settlement services in the RTGS System, for the purpose of Settlement of Net Activity in the Payment System.

- 8.2.2. The Net Activity will be settled from the relevant Clearing Accounts of the RTGS System Direct Participants.
- 8.2.3. A Payment System Participant who does not hold a Clearing Account shall be required to be represented in the RTGS System by a RTGS System Direct Participant, and the Settlement of the Net Activity Results of the Clearing Represented Participant will be carried out in its Clearing Account.
- 8.2.4. In the event that a RTGS System Direct Participant represents more than one Participant in the Payment System in the Settlement of Net Values, a single debit/credit entry will be sent to the Clearing Account of the RTGS Representing Participant, reflecting the activity of both the RTGS Representing Participant and the Participants represented in the Clearing thereby. (The entry shall be sent at RTGS Representing Participant level).

### 8.3. Types of messages to be sent from the System Operator

- 8.3.1. The System Operator shall use a single SWIFT message for the purpose of RTGS Clearing, message MT298SMT201 – this is an outgoing message from the System Operator indicating one of the following scenarios:
- 1) Clearing the System's Net Activity (multilateral transaction).
  - 2) Operation of failure event
  - 3) Request to increase collateral amounts
  - 4) Request to reduce collateral amounts
- 8.3.2. In order to distinguish between these actions, each action shall receive a different TTC (Transaction Type Code – this is an identifier number in the RTGS for the action performed). The TTC code shall be sent in the MT298SMT201 message (Tag- M99):"

Scenario	TTC code
Clearing of Net Activity	431
Reduction of collateral amount	432
Increase of collateral amount	433
Handling a failure event	434

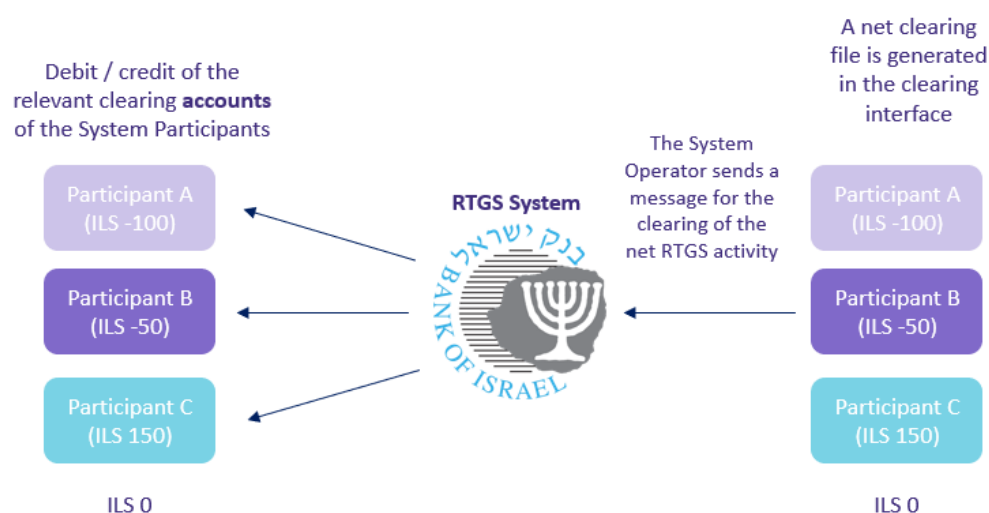
### 8.4. RTGS Clearing times

- 8.4.1. Below are details of the clearance window of the RTGS Payment System.
- 8.4.2. For purposes of completion of the Clearing, the System Participant is requested to ensure that there is a sufficient balance to complete the daily Clearing in the relevant Clearing Account during the Clearing times specified below:

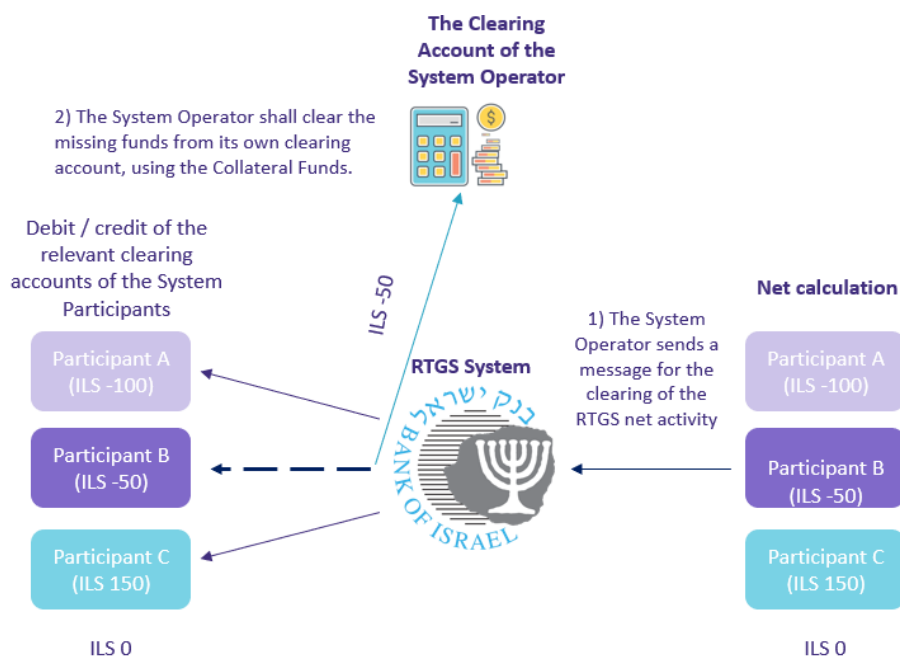
Date	RTGS Clearing time
Regular Business Day (Sunday-Thursday, Mid-holidays)	09:15-09:45
Short Business Day/Holiday eve	09:15-09:45
Saturday, Bank Holidays and holidays (both days of Rosh Hashana, Yom Kippur eve and Yom Kippur, the first and eighth day of Sukkot, Purim, the first and seventh days of Passover, Independence Day, Shavuot, Tisha B'Av, and any additional day to be defined as a non-business day by the RTGS Operator.	No Clearing

## 8.5. Description of RTGS Clearing activity

- 8.5.1. Clearing of Net Activity in the Payment System shall take place only on the days defined as Business Days in the RTGS.
- 8.5.2. The System Operator shall send a multilateral Payment Instruction to the RTGS for the Settlement of the System's Net Activity, according to the RTGS Clearing hours and days as released by the RTGS Operator on the Bank of Israel's website.
- 8.5.3. In any event where the RTGS Operator does not carry out activity on a certain day, the Settlement will be carried out on the next Business Day.
- 8.5.4. Upon receiving the RTGS Payment Instruction, the Instruction will be sent for Clearing from the relevant Clearing Accounts of the RTGS Participants.
  - 1) If there is sufficient balance for the relevant Settlement to clear the Payment Instruction of each Participant, the net Settlement will be completed immediately.
  - 2) If there is no sufficient balance for the Settlement of such Payment Instruction, the System Operator shall act in accordance with the Failure Arrangement in the Charge-Card Payment System.



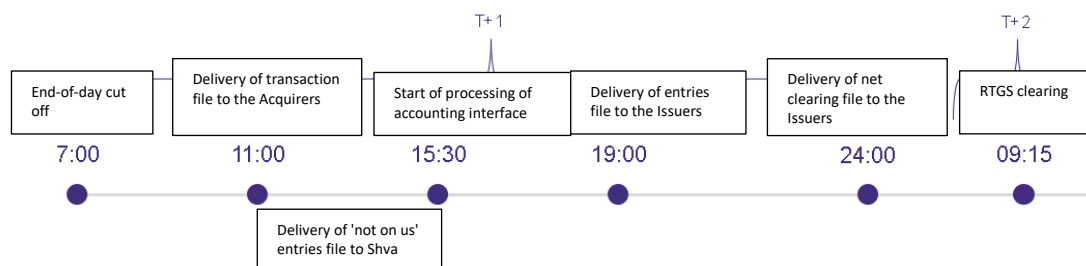
- 8.5.5. In an event as stated in Section 8.5.4(2) above:
- 8.5.6. The entire Payment Instruction will enter a pending status, and the funds intended for Settlement of the System's Net Activity will be transferred to dedicated reserve accounts in the relevant Clearing Accounts.
- 8.5.7. The RTGS System operator shall deliver in a return SWIFT message, information about the failing Participant – who it concerns and how much money is missing in the Clearing Account for completion of the Settlement.
- 8.5.8. In response (and assuming the System Operator has notified of a financial failure in the System), the Payment System Operator will send an additional Clearing message in which the TTC field contains the value 434, requesting to settle the missing amount from the Clearing Account at the Central Bank, using the Collateral Funds.
- 8.5.9. The remaining amount will be cleared from the relevant Clearing Accounts of the System Participants, using the funds transferred to the dedicated reserve accounts.



- 8.5.10. The management of a failure event will be carried out by the System Operator according to the provisions of Section 10 of these Rules, regarding the Failure Arrangement in the Payment System.

## 9. Summary Description of the System's Interfaces

Below is a summary description of the System's activity including all of its interfaces.



## 10. Failure Arrangement in the Payment System

This chapter presents the highlights of the Failure Arrangement in the Payment System.

The full arrangement is described in Annex 11 to these Rules.

It is clarified that the current full arrangement is under review and validation, and is subject to changes, which, once completed, will be released to the relevant Participants and updated in this chapter.

### 10.1 Purpose of Failure Arrangement – Ensuring the daily Settlement upon the occurrence of a failure event

- 10.1.1. The Failure Arrangement is intended to regulate the method of handling of an operational financial failure and/or financial failure (as these shall be defined below) of a System Participant.
- 10.1.2. The purpose of establishing the arrangement is to ensure the completion of the daily Settlement in the Payment System between the Issuer, as the party creating the debt in the System, and the Acquirer, such that in the event of an operational financial failure and/or financial failure of one or more System Participants, the daily Settlement shall be completed in full.
- 10.1.3. It is emphasized that the Failure Arrangement is not concerned with securing the Settlement after the date of the failure, and the funds to be provided by the Participants to secure the Settlement will be used only for the day of failure.
- 10.1.4. The Failure Arrangement concerns a failure caused by a lack of funds in the relevant Participant's Clearing Account and regulates the method of handling of such an event, but does not address any subsequent consequences, if any, between the System Participants resulting from the event.
- 10.1.5. Joining the Failure Arrangement outline is mandatory for all Participants who have signed the System Rules and/or are 'Direct Participants' who are not represented under the Rules Tier, and they are subject as aforesaid, to the terms and conditions set forth in such outline.

### 10.2. Types of failures

- 10.2.1. **"Financial failure"** – occurs when a Participant is unable to meet its obligations due to the realization of **liquidity risk** or **credit risk**;
  - 1) **"Liquidity risk"** – the risk that a counterparty will not hold sufficient funds to cover its financial obligations in the expected manner and timing, although it may be able to do so in the future.
  - 2) **"Credit risk"** – the risk that a counterparty will not be able to fully meet its financial obligations at the time of their maturity, or at any time in the future.

10.2.2. "**Liquidity failure**" – financial failure due to the realization of liquidity risk.

10.2.3. "**Credit failure**" – financial failure due to the realization of credit risk.

10.2.4. "**Operational financial failure**" – describes a situation where the Participant is technically unable to transfer funds to the relevant Clearing Account for the Settlement purpose. An "operational financial failure" shall be handled in the same manner as handling a "liquidity-type financial failure".

### 10.3. Terms for determining the type of participation

10.3.1. Directive 11 of the Supervision Directives, concerning "Participation arrangements in the system where a participant relies on the services of another participant", requires the System Operator to establish risk-based thresholds and conditions such that when these are met, participation through reliance on another Participant's services will no longer be allowed. A Type 3 or 4 Participant shall be required to become a Type 1 or 2 Participant (provided that the access conditions and System logon requirements are met). For example, in a situation where a Participant is responsible for a significant portion of the Transactions processed by the Payment System, or for a significantly large portion of the total activity of a Technical Connection Tier Representing Participant, the Participant will be required to sign the System Rules and take financial responsibility.

10.3.2. Two tests have been defined to identify a Participant that has exceeded the activity threshold:

Test	Nature of test	Significance of meeting the test
<b>Test 1</b>	A Represented Participant that is responsible for a <b>significant portion</b> of the processed transactions by the Payment System – will be required to sign the System Rules and take responsibility for its activity vis-à-vis the System Operator.	1. Upon meeting one of these two tests, a Type 3 or 4 Participant shall no longer be able to continue participating under this definition and will be required to turn into to a Type 1 or 2 Participant. 2. Transitioning from a Type 3 or 4 Participant to a Type 1 or 2 Participant means – signing the System Rules, assuming responsibility to its activity in the Payment System and participation in the Failure Arrangement.
<b>Test 2</b>	A Represented Participant that is responsible for a <b>significant portion</b> of the total activity of a Represented Participant – will be required to sign the System Rules and take responsibility for its activity vis-à-vis the System Operator.	

10.3.3. Each of the two tests has a threshold. Where a System Participant exceeds such threshold, it will be required to sign the System Rules and assume responsibility vis-à-vis the Payment System.

#	<b>A Represented Participant who relies on the services of a Representing Participant and operates through it, will be required to sign the Rules, assume responsibility for its activity in the Payment System, and participate in the Failure Arrangement</b>	
	<b>Type of test</b>	<b>Threshold value</b>
<b>1</b>	A Represented Participant, responsible for a significant portion of the transactions processed by the Payment System.	7%
<b>2</b>	A Represented Participant, responsible for a significant portion of the total activity of a Representing Participant.	40%

- 10.3.4. The method of calculation of the activity share of each System Participant for each of the tests is described in Section 4.5 of the full Failure Arrangement outline.
- 10.3.5. The activity share of a System Participant will be calculated on the 1st of March and the 1st of September each year. The calculation will take effect on the 1st of April and the 1st of October, respectively, and be based on the issuance cycles of the 12 months preceding the calculation date, provided that the System Operator is able to perform the calculation independently without relying on the System Participants.
- 10.3.6. The System Operator shall be able to set additional days for calculating the activity share of the System Participants as needed (such as a sharp change in the activity cycles and/or the subscription of a new Participant). These days shall be determined in coordination with the System Participants.
- 10.3.7. The activity share as determined on the measurement day shall remain fixed for the System Participant until the next measurement day, or until there is a change in the scope of Participants (addition/removal of a System Participant) that requires recalculation, or in the event of a one-time, extreme event in the activity cycle of a System Participant.
- 10.3.8. A Type 3 or 4 Participant who has exceeded the thresholds set above will be required to assume responsibility accordingly, and transition to a Type 1 or 2 Participant – meaning that the Failure Arrangement described in this chapter shall apply to such Participant.
- 10.3.9. The System Operator shall inform, the relevant Participants required to take part in the Failure Arrangement 30 days in advance to allow for preparation.

#### **10.4. Collateral Funds**

##### **10.4.1. Management of Collateral Funds**

- 1) The System Operator shall manage the Clearing Account at the Central Bank, where the Collateral Funds of the System Participants shall be held.
- 2) The Clearing Account at the Central Bank shall be used exclusively for management of the Collateral Funds of the Participants (Type 1 or 2 Participant) to whom the Arrangement applies. These funds will be held in escrow by the System Operator for the benefit of the Participants who deposited the Collateral Funds, for purposes of completion of Clearing upon the occurrence of a failure event as part of the Failure Arrangement, and not for any other financial activity of the System Operator.

A legal agreement is in place between the System Operator and the Bank of Israel, which defines the permitted activity in the Clearing Account at the Central Bank in such manner.



- 3) The System Participants to whom the Failure Arrangement applies (Type 1 or 2 Participants) are required to transfer Collateral Funds to be held in the Clearing Account at the Central Bank.

The funds shall be transferred on the date determined by the System Operator (Section 4.6.8.9 of the full Failure Arrangement language).

- 4) These Collateral Funds shall serve as collateral in the event of a failure event by the System Participant, so as to ensure the daily Settlement of the System Participants.
- 5) The method of calculation of the Collateral Funds shall be made on the 1st of March and the 1st of September, provided that the System Operator has the ability to identify the issuances of the Represented Participants independently, without relying on data from direct Participants. If the System Operator is unable to independently identify the issuances of the Represented Participants as mentioned, the System Operator shall contact the direct Participants to obtain the relevant data, which will be provided by the direct Participants within the specified deadlines. The amount of calculated collateral shall take effect on the 1st of October and the 1st of April, respectively, or on the next Business Day if the 1st of the month is not a Business Day.
- 6) Participants shall be given 30 days for the transfer of the Collateral Funds.
- 7) The System Operator shall update the relevant System Participants as follows:
  - 7.1 The System Operator shall send a letter signed by the authorized functionary on its behalf, as defined in **Annex A** to the full Failure Arrangement language.
  - 7.2 The letter shall be delivered by sending an e-mail to the e-mail addresses of the System Participants as defined in **Annex B** to the full Failure Arrangement language.
  - 7.3 The System Operator shall contact the relevant contacts on behalf of the System Participants and confirm receipt of the e-mail. The contact shall be made to the contacts as defined in **Annex B** to the full Failure Arrangement language.
- 8) If required, the calculation of the collateral amount will be performed at additional times as needed (for example, the subscription of a new Participant, or a sharp change in the activity of one of the System Participants). The immediacy of performing the calculation depends on the ability of Shva to perform the calculation independently without relying on the System Participants.
- 9) The System Operator shall sample, on the measurement day (as shall be defined in Section 4.6.8.3 of the full Failure Arrangement language), the amount of the Net Activity of the System after offsetting all of the System Participants who are subject to the Arrangement, and shall identify the day when the aggregate exposure of all System Participants together, is the highest. The highest aggregate exposure amount will be the collateral amount that all of the Participants together (subject to the Arrangement) will be required to transfer to the System Operator's Clearing Account at the Bank of Israel.
- 7.4 Such calculation is relevant only for the period during which Mutual Guarantees are in place between the Participants, i.e., until the necessary amendments are made to the Insolvency Law to enable use of the collateral of the failing Participant, as detailed in the full Failure Arrangement language or in other relevant act of legislation.
- 10) Time of transfer of the Collateral Funds to the Clearing Account at the Central Bank:
  - 11.1) **Upon the subscription of a new Participant** – after calculating the collateral amount, the System Participant shall be informed in accordance with Section

4.6.8.5 of the full Failure Arrangement language. The Participant shall be given 30 days to transfer the collateral. The Collateral Funds are to be transferred 14 days before the Point of No Return of the first Clearing to which the new Participant is subscribing.

11.2) A Participant that exceeded one or both of the tests as outlined in Section 4.5 the full Failure Arrangement language, and that becomes a Type 1 or Type 2 Participant – shall be required to sign the System Rules within 30 days from the notification of the System Operator regarding the change, and transfer the required Collateral Funds 14 days before the Point of No Return of the first Clearing to which the new Participant is subscribing.

11.3) **An existing participant under the Arrangement** – after determining the collateral amount of the Participant (Section 4.6.8.1 of the full Failure Arrangement language), the System Operator shall check whether the Participant's new collateral amount is higher or lower than the current collateral amount for such Participant in the System Operator's Clearing Account at the Central Bank.

The new collateral amount	Method of completion/transfer of collateral
<b>Higher</b> than the current collateral amount in the System Operator's Clearing Account at the Central Bank	<ol style="list-style-type: none"> <li>1. The System Participant shall be informed on the amount of collateral it is required to supplement as described.</li> <li>2. The Participant shall be given 30 days to supplement the collateral.</li> <li>3. The Participant shall supplement the shortfall up to two hours before the next Point of No Return of the accounting interface (the Point of No Return time as defined in the System Rules).</li> <li>4. The method of handling of a Participant who did not timely transfer the Collateral Funds is described in Section 5.2.8 of the full Failure Arrangement language.</li> </ol>
<b>Lower</b> than the current collateral amount in the System Operator's Clearing Account	<ol style="list-style-type: none"> <li>1. The System Participant shall be informed of the up-to-date amount of collateral.</li> <li>2. The System Operator shall return to the System Participant the difference between the existing amount of the Collateral Funds (deposited thereby) and the updated collateral amount that the Participant is required to deposit, provided that Participants who are required to supplement the Collateral Funds, have already transferred the funds, and in accordance with the terms outlined in the full Failure Arrangement language.</li> </ol>
<b>New Participant</b> that is required to transfer Collateral Funds for the first time	Pursuant to Section 4.6.8.9 of the full Failure Arrangement language.

#### 10.5. Notice on a failure event

As described in Section 5.2.2 of the full Failure Arrangement language.

#### 10.6. Failure Arrangement activation

- 10.6.1. In the event of a Clearing failure, the decision on the Failure Arrangement will be made by the System Operator, without consulting the Participants, in accordance with the principles set forth in the Failure Arrangement outline.
- 10.6.2. After the System Operator sends the Payment Instruction for the Settlement of the Net Activity in the relevant RTGS Clearing Accounts, a notification will be received indicating whether the Clearing was approved or rejected.
  - 1) If, in the Clearing Account, there is a sufficient balance for completion of the Settlement, the Clearing shall be successfully completed.
  - 2) If there is insufficient balance to complete the Settlement, the System Operator shall take the following steps:
    - 2.1) Contact the System Participant in whose Clearing Account are insufficient balances for completion of the Settlement – insofar as the balances are immediately supplemented (as stated in Section 2.2 below), the Clearing shall be completed with no failure event notice.
    - 2.2) It is clarified that **immediate** supplementation of the funds in the relevant Clearing Account of the Participant means supplementation of the funds immediately upon the System Operator's request and, at the latest, up to 20 minutes before the closing of the Clearing window of the Charge-Card Payment System in the RTGS System.
    - 2.3) If the balances in the Clearing Account are not immediately supplemented by the System Participant, the System Operator shall notify of a financial failure in the Payment System and take the necessary steps to supplement the Clearing (as described in Section 5.2.3 of the full Failure Arrangement).
    - 2.4) The Clearing window of the Charge-Card Payment System starts at 09:15 and ends at 09:45 on a Business day. The funds are required to be supplemented by no later than 09:25 on a Business day. If the funds are not supplemented by such time, the System Operator shall inform on the activation of a failure event.

#### 10.7. Implementation of the Failure Arrangement in accordance with the type of failure

##### 10.7.1. Liquidity failure

- 10.7.1.1. In the case of liquidity failure, the failing Participant will not have sufficient funds for completion of the Clearing in the Clearing Account relevant to the clearing of the Payment System activity.
- 10.7.1.2. The method of completion of the Clearing is dependent on the amount the failing Participant is lacking to complete the Clearing.
  - 1) If the amount missing for the failing Participant to complete the Clearing is **equal to or smaller than** the amount of its Collateral Funds, the Clearing shall be completed based on a **personal guarantee mechanism only**, as detailed below:

- 1.1) When the Clearing window of the RTGS Charge-Card Payment System opens, the System Operator shall clear the missing funds from the Clearing Account at the Central Bank and the remaining amounts from the relevant Clearing Accounts of the Participants. Information regarding the missing amount will be received through the RTGS response message to be sent back to the System Operator, which will include the details of the failing Participant and the missing amount in its Clearing Account.

The System Operator will send a **new** clearing message, and the missing amount for the failing Participant will be cleared from the Clearing Account at the Central Bank. If there is any balance in the failing Participant's account, it will be used, and only the missing amount will be cleared from the Clearing Account at the Central Bank.

- 2) If the amount that the failing Participant is missing to complete the Clearing is **higher** than the amount of Collateral Funds it deposited in the Clearing Account at the Central Bank, the Clearing shall be completed using a combination of **personal guarantee mechanism + Mutual Guarantee mechanism** as detailed below:
- 2.1) When the Clearing window of the RTGS Charge-Card Payment System arrives, the System Operator will clear the missing funds from the Clearing Account at the Central Bank and the remaining amounts from the relevant Clearing Accounts of the Participants.

Information regarding the missing amount will be received through a response message that will return to the RTGS System Operator, which will include the details of the failing Participant and the amount missing from its Clearing Account. The System Operator shall send a **new** Clearing message, and the missing amount for the failing Participant will be cleared from the Clearing Account at the Central Bank.

- 3) Completion of the Clearing through the survivors' funds shall be made as specified below:

	The Participants to whom the Failure Arrangement applies				
	Participant 1	Participant 2	Participant 3	Participant 4	
Net clearing – the highest aggregate exposure of System Participants	ILS 180M				Total collateral in the clearing account of the System Operator – ILS 180M
Issuance share out of the gross amount	40%	30%	20%	10%	
Collateral amount in ILS in millions	ILS 72M	ILS 60M	ILS 36M	ILS 18M	

#	Failing participant	Type of failure	Amount of failure	Clearing to be completed by the Participant	Division of the failure money between the Participants between the Surviving Participants
1	1	Full liquidity	ILS 40M	1	By the failing participant only
2	1	Full liquidity	ILS 90M	1,2,3,4	<p>All of the Participants, as follows:</p> <p>Participant 1 – Shall pay ILS 72M from its Collateral Funds</p> <p>The remaining amount – ILS 18M shall be divided between the Participants as follows:</p> <p>Participant 2 shall pay: <math>(40\%-100\%) / 50\% &lt; 0.5 = 30\%</math> out of 18M &lt;&lt; shall pay ILS 9M</p> <p>Participant 3 shall pay: <math>(40\%-100\%) / 33\% &lt; 0.33 = 20\%</math> out of 18M &lt;&lt; shall pay ILS 5.94M</p> <p>Participant 4 shall pay: <math>(40\%-100\%) / 17\% &lt; 0.17 = 10\%</math> out of 18M &lt;&lt; shall pay ILS 3.06M</p>

10.7.1.3. The method of completion of the Collateral Funds after a liquidity-risk type financial failure is described in Section 5.2.6 of the full Failure Arrangement language.

10.7.1.4. The System Operator shall update all System Participants regarding the Participant's failure.

#### 10.7.2. Credit failure

10.7.2.1. The Clearing shall be completed according to the **Mutual Guarantee mechanism**, in which the non-failing System Participants (the "**Surviving Participants**") shall supplement all of the missing balances for the failing Participant, if such supplementation is required.

10.7.2.2. Whether the failure is identified before or after the Clearing window, the completion of the Clearing shall be done according to the Mutual Guarantee mechanism.

10.7.2.3. The System Operator shall send a Clearing message instructing the Clearing of the failing Participant's Clearing amount from the Clearing Account at the Central Bank, meaning from the Collateral Funds of the Participants. In this case, only the funds of the Surviving Participants shall be used.

10.7.2.4. The method of completion of the Collateral Funds after credit failure, is described in Section 5.2.6 of the full Failure Arrangement language.

10.7.2.5. The System Operator shall inform the Participants in the entire System of the System Participant's failure, and shall take action for removal of the failing Participant from the Clearing as described in Section 5.2.8 of the full Failure Arrangement language.

### 10.8. Failure of an RTGS direct Participant that represents represented System Participants

10.8.1. This section describes how to deal with a case of failure of an RTGS Clearing Representing Participant that represents one or more of the Charge-Card Payment System Participants.

10.8.2. Clearing of Net Activity shall be executed from the secondary Clearing Account of the Represented Participant according to the following procedure:

Type of Failure of the Representing Participant	How to Manage the Failure
<b>Liquidity Failure</b>	1. Clearing will be supplemented by the funds of the Represented Participant pursuant to a Personal-Guarantee mechanism. 2. In case funds are insufficient, Clearing will also be supplemented by the funds of the Surviving Participants – a Mutual-Guarantee mechanism.

<b>Credit Failure</b>	<ol style="list-style-type: none"> <li>1. Clearing will be supplemented by the funds of the Surviving Participants only – Mutual Guarantee.</li> <li>2. The Participants represented by the failing Participant have not failed and therefore their funds may also be used in the interest of Clearing completion.</li> <li>3. The Participants represented for Clearing purposes by the Representing Participant that failed will be required to apply to another RTGS System Direct Participant for RTGS Clearing representation thereby.</li> <li>4. In case an RTGS Clearing Represented Participant that is represented by the failing Participant fails to apprise the System Operator of the identity of the other RTGS System Direct Participant that will be representing it for Clearing purposes <i>in lieu</i> of the failing Participant, the System Operator will be compelled to remove it from the next Clearing until it apprises of the identity of the new Participant that represents for RTGS Clearing purposes.</li> </ol>
-----------------------	--

#### 10.9. How to manage a Participant that failed

10.9.1. A Participant that failed shall be suspended from the System in the following cases:

- 1) A System Participant that failed on grounds of credit.
- 2) A System Participant that failed on grounds of liquidity and failed to timely supplement the Collateral Funds.
- 3) A System Participant that failed to supplement the Collateral Funds within the designated timeframe.

10.9.2. The System Operator shall take the following measures with respect to a suspended Participant:

Type of Participant	How to Manage a Participant that Failed
<b>Participant that failed on grounds of credit</b>	<p>The following measures shall be taken <b>immediately</b> before the next Clearing round:</p> <ol style="list-style-type: none"> <li>1. Removing the System Participant from the next Clearing round.</li> <li>2. Halting third-party interface continuous Transactions (including future payments).</li> <li>3. Blocking the POS activity of cards issued by the System Participant.</li> <li>4. Halting the activity of Businesses that clear vis-à-vis the failing Participant.</li> </ol>
<b>Participant that failed on grounds of liquidity and failed to timely supplement the Collateral Funds or survived the failure but failed to timely supplement the Collateral Funds</b>	<p>The following measures shall be taken immediately before the next Clearing round:</p> <ol style="list-style-type: none"> <li>1. Removing the System Participant from the next Clearing round.</li> <li>2. Halting third-party interface continuous Transactions (including future payments).</li> </ol> <p>Before any further measures are taken by the System Operator, the System Operator will allow the System Participant to supplement the Collateral Funds after the first Clearing round (following the failure event) from which it was removed and before the second Clearing round.</p> <p>In case a System Participant fails to supplement the missing funds before the next Clearing round as well, the System Operator will be compelled to take further measures against the System Participant:</p> <ol style="list-style-type: none"> <li>1. Blocking the POS activity of cards issued by the System Participant.</li> </ol>

	2. Halting the activity of Businesses that clear via the failing Participant.
--	---

#### 10.10. Reinstating a System Participant

- 10.10.1. The System Operator shall allow a System Participant that has been removed from System activities on Grounds 2, 3 as described in Sections 10.2.9(2) or 10.2.9(3) [10.9.1(2) or 10.9.1(3)] [ההפניה שגויה] above to resume all System activities, provided that it supplements all the missing Collateral Funds.
- 10.10.2. The System Operator will lift the restrictions described in the previous section as soon as possible.
- 10.10.3. The condition for lifting the restrictions – full supplementation of all Collateral Funds in accordance with the System Rules.
- 10.10.4. A System Participant that shall have experienced a credit failure and against which insolvency proceedings shall have been initiated may be reinstated after the receipt of a judicial decision whereby the System Participant is no longer in insolvency proceedings, provided that it complies with all the payment system rules.
- 10.10.5. After reinstatement of a System Participant that failed, the System Operator shall send an update regarding the System Participant's reinstatement to all System Participants and shall adjust the amount of the required collateral and repay the Collateral Funds to the Surviving Participants or demand funds (in accordance with the instructions in Section 4.6 of the full form of the failure arrangement).

### 11. Participation Cancellation or Participant Suspension

#### 11.1. Participation cancellation

- 11.1.1. A System Participant **may** notify the System Operator in writing of its wish to discontinue its use of the System and cease receiving System services, noting the preferred date for cancellation of its participation.
- 1) Such System participation cancellation notice shall be submitted in writing at least 60 Business Days before the preferred participation cancellation date (the "**Prior Notice**").
  - 2) The System Operator will notify the System Participant and the other System Participants shortly and, at the latest, within 7 Business Days of the date of submission of the Prior Notice, of the date of termination of its participation in the System, in accordance with its notice.
  - 3) A System Participant that wishes to terminate its participation in the System shall pay the System Operator the fees that shall have accrued in respect of use of the System and the services rendered by the System Operator to the System Participant until the date of termination of its participation in the System, which the Participant has not yet paid the Operator.
- 11.1.2. The System Operator may cancel the participation of a System Participant, stop the System Participant's use of the System and cease providing System services thereto on the following conditions:



- 1) The System Participant was suspended from System activities (in accordance with the provisions of Section 11.2 of the Rules) and 60 days thereafter, the grounds for the suspension are still in effect.
  - 2) The System Participant was suspended from RTGS System activities (in such a case, a RTGS Clearing Represented Participant represented by that Participant which was suspended from the RTGS System, if any exist, will be requested to immediately notify of another RTGS System Direct Participant that will be representing it for Clearing purposes, failing which the System Operator will halt the Clearing activities of that Represented Participant).
  - 3) A Statutory Requirement for cancellation of its participation was given to the Company.
  - 4) A Technical Connection Represented Participant ceased being represented for technical connection purposes by a Technical Connection Representing Participant and has failed to notify of its representation by another Participant or of its request to become a Participant with Direct Technical Connection.
- 11.1.3. Discontinuation of the activity of an Acquirer-type Participant (whose participation was suspended in accordance with Section 11.2 of the Rules or canceled in accordance with this section) shall be carried out in stages, as follows:
- 1) At the first stage, Clearing authorization will be deactivated in all Terminals cleared thereby and the transfer of Transaction Approval Requests on its behalf to Issuers will also be blocked (such that the “input” of Transactions into the System is stopped). At the same time, the reception of requests to activate Terminals that are cleared by the Acquirer will be discontinued, the transfer of requests to the Acquirer to confirm the activation of Terminals and the receipt of activation confirmations and updates from the Acquirer will be discontinued.
  - 2) The first stage will end after all Terminals that worked with the Acquirer being blocked contact the System and receive new Clearing authorizations and parameters and/or at the lapse of 3 months as of the blocking date (Terminal cancelation for inactivity) – whichever is earlier.
  - 3) At the second stage, collection of the Transactions and their transfer to the Acquirer shall be completed (two weeks after the end of the first stage). The Participant’s participation in the System shall be discontinued only after this stage.
- 11.1.4. Discontinuation of the activity of an Issuer-type Participant (whose participation was suspended in accordance with Section 11.2 of the Rules or canceled in accordance with this section) shall be carried out as follows:
- 1) The referral of requests for approval to the Participant shall be blocked and its cards shall be removed from the relevant vectors (such that the “input” of Transactions into the System for the Issuer’s cards is stopped).
  - 2) Blocking will be completed after all Terminals contact the System and receive the new vectors and/or at the lapse of 3 months as of the blocking date.
- 11.1.5. Discontinuation of the activity of an accounting interface Participant whose participation was suspended (in accordance with Section 11.2 of the Rules or canceled in accordance with this section) shall be carried out at the lapse of the 60 days of Prior Notice.



- 1) The System Operator shall act under the premise that discontinuation of the System Participant's activity will be executed simultaneously in the accounting interface system as well as the approvals and collection system.
- 2) As long as there are Transactions to be debited or credited which were executed prior to the blocking date, the transfer of accounting files to and from the System Participant whose participation was discontinued shall continue, with the exception of a Participant removed due to a liquidity or credit failure event which is unable to supplement the daily Settlement in the RTGS System.

#### 11.2. Participant Suspension []

11.2.1. A System Participant shall be suspended **immediately** from participation in the System, according to the sole discretion of the System Operator, and shall cease receiving services from the System Operator, upon the occurrence of one or more of the following:

- 1) It shall have ceased to satisfy any of the conditions specified in Section 2.2 of the Rules.
- 2) A Statutory Requirement for the discontinuation of its participation shall have been given to the Company.
- 3) An order for liquidation of the System Participant shall have been issued.
- 4) The System Participant shall have violated a directive that pertains to its System activities which was issued by the Bank of Israel.
- 5) As concerns an **Issuer**-type Participant:
  - 5.1) The System Participant shall have failed on liquidity or credit grounds (as described in Section 10 of the Rules or in Annex 11 to these Rules) and shall have failed to supplement the Collateral Funds.
  - 5.2) The System Participant shall have failed to transfer Collateral Funds to secure daily Clearing (as described in Section 10 of the Rules and in Annex 11 to these Rules).

11.2.2. The System Operator **may, but is not obligated to**, according to its sole discretion, suspend a System Participant from System activity and cease providing the services to the System Participant, upon the occurrence of one or more of the following:

- 1) It shall have ceased to satisfy any of the conditions specified in Section 2.2 of the Rules.
- 2) A merger has been executed between two or more System Participants – for this purpose, the suspended Participant is one or more of the target entities in the merger, with the surviving entity continuing to be a System Participant.
- 3) A motion for liquidation of the System Participant shall have been filed or the System Participant shall have adopted a voluntary liquidation decision.
- 4) A motion shall have been filed for the issuance of an order to appoint a (provisional or permanent) receiver for all or a substantial part of the assets of the System Participant, or a motion shall have been filed for appointment of a (provisional or permanent) liquidator for the System Participant, or an attachment shall have been imposed on a substantial part of its assets, or another

execution act shall have been effectuated for a substantial part of its assets – which shall not have been removed within 45 days,

- 5) The System Participant shall have ceased to manage its business, or there is a concrete reasonable risk that it will cease to manage its business.
  - 6) A motion shall have been filed for a court-approved arrangement or settlement in accordance with Chapter III of Part IX of the Companies Law, between a Participant and its creditors or shareholders (provided that the motion is not in relation to a restructuring of the share capital which, in the Company's opinion, does not adversely affect the Participant's obligations under these Rules.
  - 7) Material debts of the System Participant shall have been accelerated or the causes to accelerate the same shall have been satisfied.
  - 8) The System Participant shall have admitted in writing that it is unable to comply with its financial obligations or that there is concrete doubt as to the ability of the System Participant to comply with all of its financial obligations.
  - 9) An authorized manager or a special supervisor shall have been appointed for the System Participant.
  - 10) The System Participant shall have committed an act of fraud.
  - 11) The System Participant shall have violated any of the System Rules violation of which may affect the efficiency, stability and safety of the System and/or a System Operator instruction and/or directive that are intended to maintain the efficiency, stability and safety of the System. The System Operator may send the System Participant notice of any breach of its obligations pursuant to this subsection.
  - 12) Any case where the System Participant does not hold all the required approvals and consents, for any reason whatsoever.
  - 13) The System Participant shall have carried out no System activity for a period of 6 consecutive months.
  - 14) The System Participant shall have failed to pay the Company any payment owing thereto under these Rules, timely and fully, and 30 Business Days shall have elapsed from the date of such payment.
  - 15) The existence of material technical failures with the System Participant.
  - 16) The existence of information security problems that may risk other System Participants or the System. Furthermore, any case of concern of an information security problem or a technical disruption that might adversely affect the System or parts thereof.
  - 17) The System Participant's communication infrastructure does not allow it to communicate with the System at all, or in a secure and safe manner.
  - 18) Any other event which the System Operator deems able to affect the efficiency, stability and safety of the System.
- 11.2.3. Every System Participant undertakes to inform the System Operator of the occurrence or concern of occurrence of any of the above-listed cases immediately upon occurrence thereof.
- 11.2.4. The System Operator shall notify the System Participant of its decision to suspend the System Participant immediately and without delay when such decision is made.

Without prejudice to and/or derogating from the foregoing, the System Operator shall give advance notice to the System Participant which is considered for suspension for a period of time to be specified in the notice (according to the severity of the matter), if, in the opinion of the System Operator, suspension is not required on an immediate basis or if any harm shall be caused as a result of not giving such advance notice, in order to allow the System Participant to argue its case in order to avert suspension or rectify the matter required to be rectified and invalidate the reason that led to the intention to suspend it.

11.2.5. The following shall apply to a System Participant that is suspended from the System:

- 1) Its access to the System will be blocked and it will not be entitled to participate in the System in any form whatsoever.
- 2) It will not be entitled to a refund of the fees it paid, in accordance with the Rules, by the suspension date.
- 3) It will do everything required to change its position, in accordance with the reason that led to its suspension.
- 4) For the implications of suspension following an event of failure in the net Clearing of System activities, see Section 10.8 below.

11.2.6. The System Operator may, but is not obligated to, reverse the suspension of the System Participant, if the reason that led to the suspension is no longer effective. Such suspension reversal shall be accompanied by a suspension reversal notice to the Participant.

### 11.3. **Notice to all System Participants regarding suspension and/or cancelation of participation in the System**

11.3.1. The System Operator will notify all System Participants of the date of termination of the participation (cancelation), suspension and/or reversal of suspension of a System Participant.

11.3.2. Such notice shall be sent together with the notice to the System Participant with respect to which one of the aforesaid measures is taken, unless the System Operator believes that a concurrent notice may jeopardize any or all of the System Participants, in which case the System Operator is allowed, according to its discretion, not to send such notice concurrently, but rather subsequently and as soon as possible.

11.3.3. Notwithstanding the foregoing, in case of concern of harm to the safety of the System and/or the addition of excess risk to any or all of the System Participants, the System Operator is allowed, in consultation with Oversight of Payment Systems, not to send such notice.

## 12. **Service-Level Agreements (SLA)**

### 12.1. **System availability**

12.1.1. **The approval and Transaction collection interface** is available for communication with Terminals to respond to Transaction Approval Requests and/or Transaction collection, 24 hours a day, 365 days a year; the interface operates from two sites with active-active configuration.

12.1.2. **The Transaction processing interface** operates by batch and processing is timed as specified in Section 6 of these Rules.

12.1.3. **The accounting interface** operates by batch and processing is timed as specified in Section 7 of these Rules.

## 12.2. Service and support

12.2.1. The following table presents the contact details of the Company's functions:

Call Center	Telephone	Operating Hours
Customer Service	03-5264646	Sundays through Thursdays from 08:00 to 17:00 Fridays and holiday eves from 08:00 to 13:00
Software Support	03-5264666	Sundays through Thursdays from 08:30 to 17:00 Fridays and holiday eves from 08:00 to 12:00
Operation Room	03-5264659 03-5264660	24/7

12.2.2. Notwithstanding the foregoing, it is clarified that the binding and up-to-date contact details are posted on the Company's website.

12.2.3. The System Operator shall act within a reasonable amount of time according to the circumstances to provide operational support and respond/resolve the requests of System Participants.

12.2.4. The System Operator may change the operating hours of the call centers temporarily or permanently and may also change the nature of provision of the service (e.g., telephone call, IVR, response on the website, etc.), according to its business and technical considerations.

## 12.3. Management of failure events

12.3.1. The System Operator will manage failure events in the System according to their severity in accordance with the following table.

12.3.2. The failure will be managed continuously until the problem is resolved.

Severity of Event	Implication	Urgency
<b>Critical/Very Major</b>	1. Harm to the System's Core Activity and activities defined as services to Participants that require full uninterrupted flow. 2. Shutdown of a key process, including completion of the RTGS Clearing, or delay of integration with other systems.	Immediate
<b>Major</b>	1. Harm to the System's Core Activity and activities defined as services on a daily level 2. A failure in the performance of a process that is not dependent on other processes.	Immediate
<b>Moderate</b>	1. Harm to the System Operator's services. 2. A failure that occurs from time to time. 3. Can withstand delay.	As soon as possible
<b>Minor</b>	Harm to work processes without a damaging effect on the System Operator's services but needs to be addressed.	According to order of priorities to be determined
<b>Minimal/Very Minor</b>	Minor harm that does not affect the proper function of the System.	According to order of priorities to be determined

#### 12.4. Contact persons (System Operator and Participants)

12.4.1. **Contact persons on behalf of the System Operator** – As specified in Section 12.2 above.

The names of the contact persons will be provided to the Access Applicant according to the progress of the connection process and as necessary.

12.4.2. **Contact persons on behalf of the System Participants**

- 1) Every System Participant is required to appoint a primary contact person and a secondary contact person (as backup) to whom the System Operator will refer questions, inquiries, instructions and notices related to changes in and/or use of the System as specified in Annex 1 to these Rules.
- 2) System Participants are required to notify the System Operator of changes in the identity of the contact persons on their behalf and in their contact details within a reasonable time prior to such changes.
- 3) The (primary and/or secondary) contact persons shall be available throughout System operating hours.

#### 12.5. System Changes

12.5.1. **Changes due to Statutory Requirements**

- 1) Where the System Operator is required to make changes in the System and/or System specifications and/or services as a result of Statutory Requirements that shall apply to the Company, the System Participants' consent to the performance of such changes shall not be required. However, the System Participants shall be consulted on the manner of implementation of the requirement.
- 2) In case the aforesaid changes so made by the System Operator require (all or some) System Participants to make adjustments and/or changes and/or developments in their systems in order to allow for continued System activity and/or receipt of services, the System Participants shall make the required adjustments and/or changes and/or developments and each bear its own costs as entailed by such adjustments and/or changes and/or developments.
- 3) The System Participants shall bear the costs entailed by the performance and/or incorporation and/or implementation of adjustments and/or changes and/or developments required in the System and/or System specifications and/or services as a result of Statutory Requirements that shall apply to the Company, and all according to the manner of allocation of the costs as shall be determined by the System Operator and subject to its discretion only.
- 4) Changes performed in the System due to such Statutory Requirements shall be performed according to the target dates specified by such statutory functions.
- 5) Where the System Participant fails to make the adjustments and/or changes and/or developments required thereof due to the change in the System, this will be deemed a violation of System Rules whose violation might materially affect the efficiency, stability and safety of the System, and the provisions of Section 11.2 regarding the suspension of a System Participant shall apply.
- 6) It is the responsibility of an Acquirer System Participant to act for and ensure incorporation of the adjustments and/or changes and/or developments in all Terminals installed in the Businesses cleared thereby according to the timetable delineated and dictated by the Statutory Requirements that led to the change.

#### **12.5.2. Changes due to decisions of the EMV Protocol NGO**

- 1) Where the System Operator is required to make changes in the System and/or System specifications and/or services as a result of decisions made by the NGO with respect to mandatory components, the System Participants' consent to the performance of such changes shall not be required. However, the System Participants shall be consulted on the manner of implementation of the requirement in Participants Committees.
  2. In case the change so made requires the System Participants to make adjustments and/or changes and/or developments in their systems in order to allow for continued System activity and/or receipt of services, the System Participants shall make the required adjustments and/or changes and/or developments and bear the costs insofar as determined by the NGO and according to the target dates specified by the NGO.
- 2) As pertains to NGO decisions in relation to elective components, the provisions of Section 12.5.3 below shall apply.
- 3) Where the System Participant fails to make the adjustments and/or changes and/or developments required thereof due to the change in the System, this will be deemed a violation of System Rules whose violation might materially affect the

efficiency, stability and safety of the System, and the provisions of Section 11.2 regarding the suspension of a System Participant shall apply.

- 4) It is the responsibility of an Acquirer System Participant to act for and ensure incorporation of the change in all Terminals installed in the Businesses cleared thereby according to the timetable delineated by the NGO.

#### 12.5.3. Other changes

- 1) In any other case where a change in the System and/or System specifications and/or services provided via the System is sought, including changes deriving from the decisions of the Charge Cards Committee of the Bank of Israel/the decisions of the NGO in relation to elective components or from System Participants' need to comply with the requirements of the International Schemes (and insofar as Additional Services as defined in Section 3.7 of the Rules are concerned, subject to the provisions of that section), which affect one or more System Participants, the sought changes will be made in consultation in good faith with the relevant Participant/Participants affected by the change. For the avoidance of doubt, it is clarified that in such case as well, the System Participant's consent to the performance of such changes shall not be required. As pertains to requests for adjustments and/or changes and/or developments that derive from requirements of the International Schemes whose cards are configured in the System – the System Operator shall, in the context of the consultation, assign extra weight to the Participants' need to comply with the requirements of the schemes and the implications of noncompliance with such requirements, while considering the ramifications for the stability and efficiency of the Payment System and the Participants therein.

In case the aforesaid changes so made require any of the System Participants to make adjustments and/or changes and/or developments in their systems in order to allow for continued System activity and/or receipt of services, the System Participants shall make the required adjustments and/or changes and/or developments and each bear its own costs as entailed by such adjustments.

- 2) For the avoidance of doubt, it is clarified that the System Operator may make changes according to business technological needs, information security considerations and any other non-material consideration in the System and/or in any System component, without the System Participants' consent and even without consulting with any of the System Participants, where such change does not require any of the Participants to make adjustments in its systems or adversely affect the services provided pursuant to these Rules to any of the System Participants.
- 3) The System Operator shall conduct control over the performance of changes in the System in accordance with the following rules:
  - 3.1) The System Operator shall deliver in advance, within two weeks or thereabouts, notices and instructions to the Participants prior to the incorporation of planned changes into the System.
  - 3.2) In accordance with the changes made in the System, the System Operator shall, as necessary, make amendments to the Rules and to any other document that requires amendment.



3.3) All changes will be tested in a trial environment prior to their incorporation into the production system. System Participants may be requested by the System Operator to comply with the testing manual for the change performed, which shall be provided to them by the System Operator.

- 4) Any proposed change in the Participant's interfaces with the System requires prior approval by the System Operator. The System Operator reserves the right to refuse to approve such a change which is incompatible with the standard configuration requirements of the System.

#### **12.5.4. Changes/Developments pertaining to maintenance of the stability, efficiency and proper functioning of the Charge-Card Payment System**

- 12.5.4.1. Any decision that pertains to a development in the System, for the purpose of maintaining its stability, efficiency and proper functioning, shall require the agreement of 85% of all System Participants. However, the development costs of the solution approved shall be borne by 100% of the System Participants.

#### **12.6. Release of System changes**

- 12.6.1. Software changes in the approval and Transaction collection interface and the Clearing and accounting interface shall be released for operation in the production environment, in coordination with the System Participants.
- 12.6.2. The System Operator shall act in accordance with the foregoing, with the exception of urgent System changes according to its discretion, which shall be reported to the Participants as soon as possible.

### **13. Information Security**

#### **13.1. Information security and cyber protection standards**

- 13.1.1. Subject to Bank of Israel directives, all entities operating in Israel's Charge Card ecosystem, including the Payment System Participants, are required to comply with information security and cyber protection standards as delineated by the Bank of Israel.
- 13.1.2. The System Participant will fill out and give a statement as specified in Annex 12 to these Rules regarding its compliance with the requirements as specified below, including the provision of supporting documents.
  - 1) Presentation of a valid AOC (Attestation of Completion) for certification of compliance with PCI-DSS<sup>5</sup> **once a year**.
  - 2) **"Yuval" Supplier Assurance Questionnaire** – Once a year, completion of self-certification of the "Yuval" Supplier Assurance Questionnaire, at least at Basic Risk Level 1 (19 controls) and Certification Level B, on cyber protection and

---

<sup>5</sup> Payment Card Industry Data Security Standard (PCI-DSS).



information security, including registration for the self-assessment supplier system on the website of the Israel National Cyber Directorate<sup>6</sup>.

- 3) **Information Security Officer** – The System Participant will designate an information security officer on its behalf for information security and cyber protection purposes, including the responsibility for implementing the instructions set forth in this document.
- 4) **Information security and/or cyber protection policy** – It is the responsibility of the System Participant to ensure that it holds a supportive organizational infrastructure to properly contain and cope with incidents such as takeover of the admin account, denial-of-service attacks, intentional data corruption, data breaches and other threats.
- 5) **The Israel Cyber and Finance Continuity Center** – The System Participant will connect to the activity of and cooperate with the Cyber and Finance Continuity Center and, *inter alia*, designate a contact person, share information pertaining to cyber incidents and suspicions, exercise and implement tools and services that will be made available thereto and take action to reduce the impact of cyber-attacks and give feedback in the event of receipt of suspicious information and/or an alert from the Cyber and Finance Continuity Center.
- 6) **Resilience survey and penetrability tests** – Once a year, the System Participant will complete a resilience survey and penetrability tests for the information systems on its premises, including documentation retention and presentation. If negative findings arise in the survey or tests, the System Participant is required to set a reduction plan and timetables for addressing all findings.
- 7) **Procedures and log documentation** – The System Participant is required to devise a set of procedures for the documentation of logs and information that are related to Charge-Card activity, retain such information for a period of two years at least, and present it to the extent required.
- 8) **Secure development** – It is the responsibility of the System Participant to conduct development processes that are based on secure development best practices. Insofar as developments are written and/or executed through a third-party, it is required to ascertain that they have undergone code review processes.
- 10) **Protection of end-stations and servers** – The System Participant is required to protect the computer which is connected to the internet by standard means and run ongoing security updates in the operating system. If security updates are required, the level of severity of which is major and critical, it will run the updates immediately. For the avoidance of doubt, a point-of-sale cash register is deemed to be sensitive hardware and should not connect to the internet, other than according to the minimal business needs required for the ongoing business

---

<sup>6</sup> An explanation about the Israel National Cyber Directorate's "Yuval" Supplier Assurance Questionnaire and the questionnaire file in Excel format are available at: <https://www.gov.il/en/pages/querysupply>.

operations. If internet access is required, the System Participant is required to ascertain that it is done by 'safe browsing'.

- 11) **Credibility checks** – It is the responsibility of the System Participant to conduct credibility checks for all employees who will be working directly with the System, including documentation of the checks and presentation thereof on demand.
  - 12) **Response to distributed denial-of-service attacks (DDoS)** – If the System Participant externalizes services for endpoints as part of the payment operations, it is required to address and provide an appropriate level of protection against infrastructural and applicative denial-of-service attacks as part of the Payment System's business continuity process.
  - 13) **Authorizations** – The System Participant is required to ensure that authorizations are given to its employees on a need-to-know basis. Furthermore, the System Participant is required to exercise control over and document its employees' departure, transfer, setup and remote access processes, including retention of authorization and control records and presentation thereof to the extent required.
  - 14) **Employee awareness** – The System Participant shall conduct awareness training for its employees on information security issues, at least once a year, including attendance monitoring, and shall document training sessions and the identity of the participants therein.
  - 15) **Drills** – The System Participant shall conduct a periodic drill for employees and a periodic drill for the management of the organization.
- 13.1.3. The System Participant shall notify the System Operator immediately upon the occurrence of an information security and/or cyber incident in its systems and/or in case of concern of the occurrence of such incident.

### 13.2. Confidentiality in the ongoing work process

- 13.2.1. Without derogating from the provisions of the letter of undertaking to maintain confidentiality signed by every System Participant (in the form attached as Annex 2 to these Rules), every party to the System (the System Operator; and the System Participants, jointly and severally) as well as the RTGS Clearing Representing Participant undertakes that it and its employees and/or anyone on its behalf (the "**Receiving Party**") shall maintain in confidence any information provided to them by the other party (the "**Disclosing Party**" and the "**Information**", respectively), including information pertaining to entities and institutions that receive services from the Disclosing Party, and shall not provide the information to others or make use thereof other than for the purposes of their engagement, unless the Disclosing Party shall have given its consent.
- 13.2.2. The foregoing shall not apply if the Information is information that is publicly available other than as a result of breach of any obligation by the Receiving Party and/or information that was developed by the Receiving Party and/or anyone on its behalf on their own without any dependence and without any reliance and does not include the Information and/or information that was held by the Receiving Party and/or anyone on its behalf prior to the transfer of the Information and it holds written evidence thereof and/or is professional knowledge, generic tools, know-how,

standard tools, ideas, concepts, methodologies and work methods, which are not unique to the Disclosing Party.

- 13.2.3. Each party shall notify the other party immediately upon learning of concern of leak of information provided thereto by the other party.
- 13.2.4. At the request of the System Operator, the System Participant and/or the RTGS Clearing Representing Participant shall return thereto, immediately upon its first demand, all the documents provided thereto thereby and/or by anyone on its behalf for the purpose of its connection to the System and/or its activity as an RTGS representing Participant.
- 13.2.5. Furthermore, it is agreed that in a case where the Receiving Party and/or anyone on its behalf is subject to a duty by law and/or pursuant to Statutory Requirements and/or a court order to disclose the Information, the Receiving Party and/or anyone on its behalf may disclose the Information, provided that prior notice is given thereof to the Disclosing Party such that the option to take any measure and/or action to prevent the disclosure of the Information is available thereto, subject to there being no impediment to the giving of such notice to the Disclosing Party under any law and/or order and/or the Statutory Requirement and to the disclosure of only the minimal relevant part of the Information and to the extent required in accordance with the provisions of the law.

### 13.3. Responsibility of System Operator

- 13.3.1. The System Operator shall meet the information security standards generally accepted in the banking industry in Israel (Proper Conduct of Banking Business Directives, relevant legislation, instructions by various regulatory supervisory functions, etc.).
- 13.3.2. **Management of cyber incidents** – The System Operator shall follow the directives of the Bank of Israel pertaining to cyber protection, *inter alia*, the gamut of the acts for preventing, neutralizing, investigating and dealing with cyber threats and cyber incidents and for reducing their impact and the damage they cause.
- 13.3.3. **Procedures and log documentation** – The System Operator manages logs related to the operations and information security, which are required for the purpose of control over the System activity. Logs are kept for inquiries, the management of failure events and information security and cyber incidents for a one-year period.
- 13.3.4. After prior coordination with the System Operator, the System Operator will allow every System Participant access to maintenance of its equipment 24 hours a day.

### 13.4. Responsibility of System Participants

- 13.4.1. Without derogating from the responsibility of Bank of Israel-supervised System Participants to follow the Proper Conduct of Banking Business Directives and the specific legislation for banking entities, the System Participants shall be subject to the following provisions. In any case of discrepancy between these provisions and Bank of Israel directives, the provisions of the Bank of Israel directives shall prevail.
- 13.4.2. System Participants are responsible for performing the following:
  - 1) **Security checks** – The System Participant's Security Officer is responsible for conducting background checks for System Participant employees that will work

directly with the System, and all in accordance with Bank of Israel directives or the directives of the relevant regulator of Participants on this matter.

- 2) **Physical security** – The System Participant's Security Officer is responsible for taking appropriate protective measures to protect the premises of the Participant where System-connected end-stations are installed and/or any other place that holds information and/or access to information of and/or about the System, in such manner as shall be no lesser than the protective measures taken by the Participant with respect to its own systems.
  - 3) **Access control** – System Participants shall use technological means such as the following: A technology that integrates user identification and verification, data confidentiality and integrity and Transaction dispute prevention (e.g., smart cards, biometric identification, and so forth) for the purpose of access control over the System Participant's System-linked information systems, all as shall be dictated to the Participants from time to time by the System Operator.
  - 4) **Internal audit** – System Participants are required to integrate an audit of their System-linked internal system in their internal audit plans, and to ascertain compliance with the aforesaid conditions.
  - 5) **Survivability** – System Participants are required to establish a backup and recovery plan for the Participant's system and for the System-linked information systems.
- 13.4.3. System Participants shall ensure that their systems and procedures provide appropriate protection against malicious activities related to the System activities.
- 13.4.4. Every System Participant is responsible for the information security of the system held thereby in accordance with all the Statutory Requirements and considering the sensitivity of the information being transferred.
- 13.4.5. Any suspected or actual violation of System information security requirements shall be promptly reported to the System Operator.
- 13.4.6. Any suspected threat or cyber incident that may affect the proper operation of the System shall be promptly reported to the System Operator.
- 13.4.7. Every System Participant shall independently evaluate the reliability and resilience of its internal arrangements in relation to the security of the System-linked information systems. Such self-assessment shall include issues such as:
- 1) Physical security of the site.
  - 2) The prevalence of incidents related to operational risk, such as the shutdown time of such information systems.
  - 3) Adequacy of the message transmission rate.
  - 4) Adequacy of emergency tools and procedures.
- 13.4.8. In case gaps in relation to the System are detected during the performance of the evaluation, the System Participant shall act to close the gaps as soon as possible.
- 13.4.9. The System Participant shall report to the System Operator of any gap that affects or might affect the operation of the System.
- 13.4.10. A self-evaluation report shall be submitted to the System Operator per demand.

## 14. Risk Management

### 14.1. Responsibility of System Participants

- 14.1.1. Without derogating from the responsibility of the System Operator and the responsibility of System Participants as set out in these Rules, a System Participant bears the full and exclusive responsibility for risks transmitted thereby into the System, which arise from its activity, the activity of its customers in the System and the activity of the Participant represented thereby and its customers which operate through it in the System. No claim by a Participant shall be accepted whereby it bears no responsibility for any of the actions of the Participant represented thereby (also for an activity configuration where the Represented Participant operationally connects directly to the System) which shall have caused damage and/or loss and/or liability and/or an expense and/or demand and/or claim to the System and/or to Shva.
- 14.1.2. A System Participant shall maintain the risk management system required for operating vis-à-vis the System and shall train manpower with the expertise to manage the risks in the operation vis-à-vis the System, the parameters of which shall be no lesser than as required of the Participant by the supervising body thereof.

### 14.2. Responsibility of System Operator

Compliance with the Statutory Requirements applicable to the Company and with these Rules.

## 15. Business Continuity

### 15.1. System availability

The availability of the System is described in Section 12.1 above.

### 15.2. Basic business continuity management requirements

- 15.2.1. Subject to Bank of Israel directives, all entities operating in Israel's Charge Card ecosystem, including the Payment System Participants, are required to comply with basic business continuity management requirements as delineated by the Bank of Israel.
- 15.2.2. The System Participant will fill out and give a statement as specified in Annex 13 to these Rules regarding its compliance with the requirements as specified in this document.
- 1) **Business Continuity Officer** – The System Participant shall designate a business continuity officer on its behalf for the purpose of managing business continuity, including the responsibility for implementing the instructions specified in this document.
  - 2) **Identification of threats and processes** – The System Participant shall identify threats that have the potential to expose its systems to risks and disruptions, and it shall map out processes that are critical to payment operations and the resources required (such as related systems, measures, infrastructure, and the like).
  - 3) **Business Continuity Plan** – The System Participant shall formulate a business continuity plan to ensure functional continuity under disruptions, including

backup and recovery processes for the information systems on its premises which are related to its payment operations.

- 4) **Event reporting** – In case of an emergency or irregular operational event (including cyber), the System Participant shall report the details of the emergency event to the System Operator within two hours of the moment of commencement of the event. The System Participant is required to prepare an event debrief within seven Business Days after commencement of the event.
- 5) **Infrastructure provider** – The System Participant shall ensure its ability to replace an internet infrastructure provider within a short amount of time in the event of failure with its internet infrastructure provider. System Participants that provide payment services to “enterprises for the provision of essential services”, such as food manufacturing factories, fueling stations, airports, emergency services and the like (“**Essential Services**”) shall ensure the ability to automatically switch between 2 point-to-point connections of 2 MB each in the event of failure.
- 6) **Service provider** – The System Participant shall ensure its ability to replace an internet service provider within a short amount of time in the event of failure with its internet service provider. System Participants that provide Essential Services shall ensure the ability to automatically switch between service providers in the event of failure.
- 7) **Communication backup** – The System Participant shall ensure internet or cellular information backup ability and essential information recovery ability in the event of failure.
- 8) **Bandwidth** – The System Participant shall set a bandwidth that accounts for the volume of Entries and market changes expected therefor and shall maintain a bandwidth no lesser than 150% of its peak activity volume.
- 9) **Monitoring and control** – The System Participant is required to conduct ongoing monitoring of the proper functioning of the communication lines and bandwidth.
- 10) **Energetic backup** – A System Participant shall prepare for energetic backup in the event of a power outage (UPS, generation, and the like).
- 11) **Business continuity survey** – A System Participant shall examine, once a year, the degree of its readiness to deal with business continuity events as specified in this chapter.
- 12) **Employee awareness** – The System Participant shall conduct business continuity awareness training for its employees, at least once a year, including attendance monitoring, and shall document the training sessions and the identity of the participants therein.
- 13) **Drills** – The System Participant shall conduct a periodic drill for employees and a periodic drill for the management of the organization.

### 15.3. Responsibility of System Operator

- 15.3.1. The System Operator’s business continuity management shall be conducted in accordance with Bank of Israel directives and in accordance with Israel Emergency Economy (IEE) directives.

- 15.3.2. The System Operator shall operate a backup site in accordance with its policy and subject to Bank of Israel directives.
- 15.3.3. In the event that circumstances warrant the transfer of the System to the backup site, the System Operator shall notify the System Participants of any action that they are required to take in connection therewith. Transfer to the backup site shall be transparent, to the extent possible, to the System Participants.
- 15.3.4. In the event of prolonged shutdown of the System, the System Operator shall consult and communicate with the System Participants as necessary.
- 15.3.5. The System Operator shall give notice to the System Participants where it is likely that the problem will continue or that it might disrupt the entire System activity.

#### **15.4. Responsibility of System Participants**

- 15.4.1. The System Participants shall act to ensure their business continuity to maintain the ongoing processes vis-à-vis the System Operator from each one of the System Participant's sites to each one of the System Operator's sites.
- 15.4.2. The System Participant shall conduct testing and drills of the aforesaid activity ability at least once every two years.
- 15.4.3. A System Participant that shall have encountered problems that may prevent it from operating vis-à-vis the System is required to notify the System Operator thereof as set out in Section 1.15 of these Rules.
- 15.4.4. Survivability requirements at the Participant's site:
  - 1) System Participants are required to ensure means of survivability as pertains to the components by means of which they interface with the System.
  - 2) System Participants are required to ensure local survivability means at the primary site.
  - 3) System Participants are required to ensure remote survivability means, i.e., a backup site in case of collapse of the primary site.
  - 4) The System Operator reserves the right to relax this requirement for a Participant considering the level of the risk to which the Participant exposes the System.
- 15.4.5. In case a System Participant needs to switch to its backup site for any reason whatsoever, it is imperative that it has the ability to do so without affecting the other System Participants or the System Operator. The System Participant shall notify the System Operator immediately both of its intention to relocate operations to the backup site and of the success of the switch. The System Participant shall notify the System Operator of a switch back to the primary site.

#### **15.5. Examination of emergency procedures**

- 15.5.1. The System Operator shall examine from time to time the adequacy of its procedures for System emergencies on a periodic basis in accordance with its policy documents.
- 15.5.2. System Participants are required to cooperate and take part in this process to the extent required by the System Operator.



- 15.5.3. A System Participant shall examine from time to time the adequacy of its emergency procedures as being in place therewith on a periodic basis in accordance with its policy documents.
- 15.5.4. A System Participant shall notify the System Operator of the findings of an emergency procedures' examination that may affect the ability of the Participant to operate in the System.

## 16. Dispute Resolution

### 16.1. Competent court and governing law

- 16.1.1. The court vested with the jurisdiction for adjudication of claims between the System Participants and the System Operator (including a claim to which the Company is a party in its capacity as System Operator) on a matter regulated by the Rules or by agreements with the Participants is an Israeli court in the Tel Aviv District.
- 16.1.2. The law applicable in such cases is Israeli law and no Participant nor anyone on its behalf shall argue for the applicability of a foreign law.

### 16.2. Disputes between System Participants amongst themselves

- 16.2.1. Where a dispute arises between System Participants in relation to a Payment Instruction, Settlement or any other event that pertains to System activities, including a dispute deriving from a different interpretation of the Rules and/or agreements with Participants, the parties to the dispute shall do everything in their power to try to resolve the dispute independently, within 7 Business Days at most as of the date on which the parties to the dispute learn of the dispute.

## 17. Property Rights and Restriction of Use

### 17.1. Ownership of property

- 17.1.1. Shva owns the rights in the System and in the Rules with their annexes.
- 17.1.2. Shva is the System Operator.
- 17.1.3. It is hereby agreed that the System (with the changes thereto from time to time), which includes the software components and the System infrastructures (including the physical hardware systems), including any development and/or upgrade and/or addition thereto, all the services under these Rules, the Basic Services and the Additional Services and including the Rules with their annexes, are and shall remain the exclusive property of Shva, and no Participant and/or no party shall have any right in the System and/or in the foregoing, whether developed for a specific Participant or developed for all the Participants.
- 17.1.4. For the avoidance of doubt, it is hereby clarified that nothing in these Rules shall transfer Intellectual Property Rights or any rights, including rights of use and/or ownership of the System, the data included therein, the databases and/or specifications as noted and/or the software components of the System Operator. The term "**Intellectual Property Rights**" shall be construed as broadly as possible under the law, and, without derogating from the generality of the foregoing, the term shall include copyright, trademarks, graphic designs, patents, trade secrets, domain names and ideas, regardless of whether or not they have been registered.



17.1.5. It is hereby agreed that the work and services performed and/or provided and/or to be performed and/or to be provided and/or additional services provided and/or to be provided to (all or any of the) System Participants, either at the explicit request of the Participants or where the development and/or service is provided by Shva of its own initiative, as well as any product and/or development and/or intellectual property whatsoever in connection with the System and/or developed and/or to be developed and/or obtained and/or to be obtained and/or discovered and/or to be discovered during the performance of the work and/or services, shall be fully and irrefutably owned by Shva.

#### 17.2. Restriction of use and transferability

A System Participant may not directly or indirectly carry out all or any of the following acts: (1) sell, grant a license (or sublicense), lease, market, distribute, assign, transfer or pledge its rights to use the System without Shva's prior written approval; (2) use Shva's name, logo or trademarks without Shva's prior written approval.

### 18. Force Majeure and Limitation of Liability and Indemnity

#### 18.1. Force Majeure

The Company shall bear no responsibility and/or liability for its actions as System Operator due to events that are not within the Company's control, where despite reasonable efforts the Company could not have complied with its obligations, and without derogating from the generality of the foregoing, *inter alia*, due to any of the following events: War, threat of war, hostilities, acts of terrorism, riots or other serious security incidents, fires, floods, snow or other natural disasters, labor disputes, including strikes, lockouts and industrial actions, technical malfunctions in System computers and/or communication lines and/or System interfaces and/or power outages and/or other unavailability/dysfunctionality of other infrastructures/means that are required for performance of the activities in the System.

#### 18.2. Limitation of liability

18.2.1. The liability of the Company and those acting on its behalf is strictly limited to the provisions of these Rules. The Company and those acting on its behalf shall bear no responsibility whatsoever nor liability for any act and/or omission and/or damage due to and/or relating and/or arising from the Company's capacity as System Operator and/or from its actions under these Rules, except where all the following conditions are satisfied on a cumulative basis: (1) Such act and/or omission by the Company and/or those acting on its behalf, as applicable, was committed deliberately or in gross negligence, and (b) The damage caused as a result of such act and/or omission by the Company and/or those acting on its behalf, as applicable, is strictly direct damage and not consequential or indirect damage, and (c) The amount paid by the Company for the damage caused to a System Participant and/or another third party as a result of such act or omission committed by the Company and/or those acting on its behalf, as applicable, shall not exceed ILS 200,000.

18.2.2. The Company, its employees, managers and/or anyone on its behalf shall not be responsible nor bear any damage and/or expense and/or loss caused as a result of non-approval of the withdrawal of funds from the account of the System Participant for any reason whatsoever by the Bank with which the System Participant's account is managed, in consequence of which the other Participants are not credited for Transactions cleared through the Clearing interface.

18.2.3. The Company is not a party to the Transactions transmitted through it, does not guarantee the completion of the Settlement carried out based on the activity transmitted through it, and accordingly does not assume credit and/or liquidity risks that arise from the activity of the Participants by means of its System and/or other System users, nor assumes any liability (whatsoever) in relation to acts and/or Transactions that are carried out between the Business, the Charge Card Holder, the Issuer and the Acquirer.

#### 18.2.4. Indemnification by System Participants

- 1) Every System Participant undertakes to compensate and/or indemnify the Company in accordance with a judicial decision for any expense and/or damage and/or loss (including costs, expenses and attorney fees of a reasonable amount) incurred by the Company as a result of a claim and/or demand by a System Participant and/or third party against the Company (including by Businesses, owners of Terminals installed with any Businesses, Charge Card Holders and/or Participants and other users), in connection with the provision of the services and/or System activity.
- 2) Without derogating from the generality of the provisions of the above section, as relating to an Acquirer which is a System Participant, the Participant undertakes to compensate and/or indemnify the Company, including for a claim in respect of: (a) Failure and/or disruption and/or error in the reception of the parameters and authorizations configured for the Company by the Acquirer Participant in the System; and/or (b) Failure in the Terminal in the reception of the parameters and authorizations configured for the Company by the Acquirer Participant; and/or (c) Engagement of the Acquirer Participant with any Business following which that Business terminates the engagement of the Business with another System Participant.
- 3) Without derogating from the generality of the provisions of the above section, as relating to an Issuer which is a System Participant, the Participant undertakes to compensate and/or indemnify the Company, including for a claim in respect of: (a) Failure and/or disruption and/or error in the reception of the vectors configured for the Company by the Issuer in the System; and/or (b) Failure in the Terminal in the reception of the vectors configured for the Company by the Issuer.
- 4) A System Participant that represents a Type-4 Represented Participant in one or more access tiers shall be fully and exclusively responsible for the fulfillment of such Represented Participant's obligations at the standards of information and cyber security and business continuity, in accordance with the Statutory Requirements applicable to such Represented Participant.
- 5) Without derogating from the generality of the provisions of the above section, as relating to a Representing Participant which represents a Represented Participant, the Representing Participant undertakes to compensate and/or indemnify the Company for any expense and/or damage and/or loss (including, costs, expenses and attorney fees of a reasonable amount) incurred by the Company in relation to and/or as a result of the acts and/or failures to act of the Represented Participant in the System and/or the Representing Participant in the System on behalf of the Represented Participant, at the relevant representation tier, and for any breach of any and/or all of the duties, requirements and obligations applicable under the System Rules and/or their annexes in relation to

the activities of the Represented Participant or the Representing Participant in the System on behalf of the Represented Participant at the relevant representation tier, and for any third-party claim and/or demand against the Company (including by Businesses, owners of Terminals installed with any Businesses, Charge Card Holders and/or Participants and other users), in connection with the Represented Participant, including the acts of the Represented Participant and its customers that operate via the Represented Participant in the System (even where the Represented Participant is operationally connected directly to the System, and including in connection with the foregoing provisions of Section 18.2.4(4) on the obligations of a Type 4 System Participant) and in connection with all the duties, requirements and obligations applicable under the System Rules in relation to the activity of the Represented Participant).

- 6) The Company shall notify a System Participant in writing, as soon as possible, of any such written demand and/or claim and allow it to defend itself against it. The System Participant may not cause the conclusion of the aforesaid proceeding by way of a settlement or compromise as a result of which any liability is imposed on the Company and/or the Company is required to pay amounts for which it will not be indemnified under this indemnity clause, other than with its prior written consent thereto. A System Participant shall not admit to any culpability (including on behalf of the Company) without the prior written approval of the Company.
- 7) The Participant bears full and exclusive responsibility for all the risks transmitted thereby onto the System, including credit and liquidity risks, regulatory risks and money laundering and terrorism financing risks that arise from its activities, the activities of its customers in the System and the activities of the Participant represented thereby and its customers which operate through it in the System. The aforementioned applies to any activity configuration under which the Participant operates.

## 19. System Users and Other Engagement Configurations

- 19.1. This section below presents a merely general and concise description (which does not constitute an “exhaustive list”) of certain entities that use the System services and are not System Participants, including their activities in connection with the Charge-Card Payment System:

### 19.2. EMV software manufacturers

- 19.2.1. An EMV Software Manufacturer as defined herein is a System Participant.
- 19.2.2. EMV Software Manufacturers may connect the Terminals they market to the System upon satisfaction of the following conditions:
  - 1) Signing a manufacturer agreement that regulates the relationship between the parties.
  - 2) Approval of the Terminal for operation vis-à-vis the System by a function authorized for this purpose.
  - 3) Technical and security approval of the connection of the Terminal by the System Operator.

- 19.2.3. EMV Software Manufacturers may market the Terminals approved for connection and operation vis-à-vis the System via software distributors.

#### 19.3. Pin-Pad marketers

- 19.3.1. Entities that provide hardware components that allow for the pin code to be typed-in and verified against the Charge Card when an EMV Transaction is made.

#### 19.4. Payment Gateway

- 19.4.1. A Payment Gateway, as defined herein, concentrates the activity of various endpoints by means of a server/cloud and serves as a router for the approval requests and Transaction transmissions vis-à-vis the Payment System, and it is a System Participant.
- 19.4.2. Each one of the endpoints operating via a Payment Gateway has its own specifically assigned Terminal number.
- 19.4.3. Transaction transmission will be carried out from every endpoint and include all the Transactions made at that endpoint which relays the transmission. Namely, Transactions will be transmitted via separate files for the activities of all the endpoints.
- 19.4.4. Every endpoint shall receive its own Blocked Card Files and parameters file from the System Operator.

#### 19.5. Credit reconciliation/factoring companies

- 19.5.1. A factoring company is an entity that provides services for advancing credit payments (discounting) to Businesses before the scheduled date for receipt of the payment from the Acquirer, provided that the corporation holds a credit service provision license granted by the Israel Capital Market, Insurance and Savings Authority under the Control of Financial Services Law (Regulated Financial Services), 5776-2016.
- 19.5.2. The essence of the service is that the factoring company “steps into the shoes of the Business”, such that the factoring company receives from the System Participant (Acquirer) the payments intended to be transferred to the Business (“assignment of rights”).
- 19.5.3. To that end, in every Transaction (for which substitution of the Business for the factoring company has been requested) the System Operator endorses the details of the Business in which the Transaction was made with the details of the factoring company.
- 19.5.4. This service requires advance written agreement between the factoring company, the (Acquirer-type) System Participant and the System Operator.
- 19.5.5. The factoring company shall submit to the System Operator a request approved by the Business and the Acquirer with which it has entered into an agreement for assignment of the rights for every Business that requests to be included in the service, specifying the types of Transactions for which factoring shall be performed.
- 19.5.6. The System Operator shall execute the assignment of rights in every Transaction record in accordance with the aforesaid requests and settings, prior to transfer of the Transaction records to the Acquirer System Participant. The System Operator shall further forward to the factoring company a copy of the factoring-endorsed Transaction records for all the Acquirers in all the Businesses engaged with the factoring company.

19.5.7. The factoring company may also submit to the System Operator requests for a Business's removal from, attribution to or disconnection from the factoring service only.

#### **Credit reconciliation companies**

19.5.8. Credit reconciliation companies are entities that provide control and reconciliation services between debits and credits recorded by the Business and the consideration actually received in respect thereof from the Acquirer.

19.5.9. The System Operator may operate vis-à-vis credit reconciliation companies that are certified for the provision of credit card control and reconciliation services to Businesses.

19.5.10. The credit reconciliation company shall submit to the System Operator a request approved by the Business, for every Business that requests to be included in the service. This service requires the System Operator's advance written consent.

19.5.11. The System Operator shall perform the update in accordance with the aforesaid request and forward to the reconciliation company, on a daily basis, a copy of the file of Transactions that are relevant to the Business included in the service.

19.5.12. The Transaction files will be forwarded to the reconciliation company in a secured manner by means of the vault system.

#### **19.6. Additional engagement configurations**

An entity that wishes to operate in any of the following engagement configurations, is required to conduct prior coordination with the System Operator and with the relevant System Participants, respectively:

##### **19.6.1. Multi-Beneficiary**

- 1) Multi-Beneficiary use is intended for Businesses that manage several different beneficiaries/Suppliers.
- 2) The Multi-Beneficiary represents several Businesses ("**Beneficiaries**") vis-à-vis Acquirers.
- 3) The activation of a new Terminal for operation under this work configuration requires written approval by all the Acquirers relevant to the Terminal.
- 4) All the parameters and caps are managed at the Multi-Beneficiary Terminal level and will be shared by all Beneficiaries (endpoints) under the Multi-Beneficiary.
- 5) The leading Terminal shall be the only Terminal identified by the Payment System. This means that endpoints operating via the leading Terminal will also be identified by the leading Terminal.
- 6) When executing End-of-Day Communication, the following actions will be taken:
  - 6.1) The leading Terminal will receive a Blocked Cards File and one parameters file from the System Operator. Namely, these files will be transferred only once for the leading Terminal, rather than for each endpoint separately.
  - 6.2) Transaction transmissions from the leading Terminal will include the Transactions made at all endpoints. Namely, Transaction transmission shall not be conducted via separate files for the activity of all the endpoints separately.

### 19.6.2. Multi-Supplier

- 1) Multi-Supplier use is intended for Businesses that manage several Terminals on one server (Beneficiaries/Suppliers) with the Acquirers crediting each Beneficiary/Supplier separately.
- 2) The activation of a new Terminal for operation under this work configuration requires written approval by all the Acquirers relevant to the Terminal.
- 3) All the parameters and caps are managed at the level of every Beneficiary/Supplier separately.
- 4) The leading Terminal and the endpoints operating by means thereof shall be identified by the Payment System.
- 5) When executing End-of-Day Communication, the following actions will be taken:
  - 5.1) The leading Terminal will receive one Blocked Cards File from the System Operator. Namely, this file will be transferred once only for the leading Terminal and not for every endpoint separately.
  - 5.2) Every endpoint shall receive a Blocked Cards File from the System Operator. Namely, this file will be transferred to every endpoint registered under the leading Terminal.
  - 5.3) Transaction transmissions shall be conducted from every endpoint and include the Transactions made at the same endpoint that conducted the transmission. Namely, transaction transmission shall be conducted via separate files for the activity of all the endpoints.

**It is clarified that the System Operator does not have an engagement agreement vis-à-vis the Businesses and bears no responsibility to the Businesses and/or the Charge Card Holders. All the acts performed between the System and the Businesses are part of the range of the Company's services to the System Participants and the responsibility with respect thereto is borne fully and exclusively by the Participants themselves.**

## 20. Costs/Administration/Miscellaneous/Issuance of Test Cards

### 20.1. Fees and pricing of System operations

#### 20.1.1. Current operation costs

- 1) Fees related to use of the System shall follow the Company's rates as determined by the System Operator and as practiced by the Company from time to time.
- 2) Current fee rates are posted on the Company's website ("**Official Rates**"). The Official Rates will present the activity being charged, the basis of the charge, the payor, the amount and explanatory notes with respect to the calculation method and/or the allocation of the charge between the System Participants.
- 3) By the 5<sup>th</sup> day of every month, the Company will furnish the System Participant with a lawfully prepared tax invoice that lists the total fees accrued in its debit during the previous month (from the 2<sup>nd</sup> day of every month to the 1st day of the following month – inclusive) for services rendered thereto by the Company during such preceding month.

- 4) The System Participant's payment to the Company shall be carried out according to such payment terms as specified in the Official Rates.
- 5) As relating to the use of Basic Services, the Company shall provide Participants with files specifying the current charges in relation to use of the System.

#### **20.1.2. Cost of connection of a Participant with Direct Technical Connection**

- 1) The Access Applicant is responsible for carrying out, at its own expense, the installations, training and required maintenance and for performing any other act required for the purpose of its joining and/or using the System.
- 2) The System connection cost to be paid to the Company shall be calculated based on work hours actually dedicated by the Company and on additional costs that are required on the Company's part including external parties in connection with the System connection and which arise from the performance of the necessary adjustments for the Access Applicant to connect to the System (including all costs and expenses in connection with the provisions of Section 2.9 of the Rules). Such costs will be paid every month based on the hours and costs actually incurred. The hourly rates of the Company only will be as specified in the Company's rates on the Company's site.
- 3) Value added tax at the lawful rate at the time of payment will be added to the aforesaid payment. It is clarified that payments will be made in shekels only.
- 4) The System Operator shall provide the Participants with a file for information and control of the accounting therewith.

#### **20.2. Payment of interest**

- 20.2.1. Where any payment is not paid to the System Operator pursuant to these Rules by a System Participant at the time scheduled for payment thereof, including and without derogating from the generality of the foregoing, in respect of current costs and/or development costs and/or connection costs and/or Basic Services and/or Additional Services and/or any other services and/or changes in the System and/or changes in the Rules and in respect of Sections 1.9, 3.7, 12.5, 20.1 of these Rules, the payment will bear the Bank HaPoalim interest rate for overdrafts at that time from the scheduled payment date, which interest shall accrue on a monthly basis until the actual payment date.

#### **20.3. Financial penalty**

- 20.3.1. Without derogating from the provisions of these Rules, the System Operator may impose a financial penalty of ILS 10,000 for any violation of the System Rules and/or the failure arrangement outline, including and without derogating from the generality of the foregoing, failure to pay the System Operator any payment at the time scheduled for payment thereof, failure to meet the timetables scheduled for going live for adding a new Participant to the System as specified above in Section 2.9.3 of the Rules.
- 20.3.2. The System Operator may impose a financial penalty of ILS 50,000 for a recurring and/or continuous and/or material violation of the System Rules and/or the failure arrangement outline.
- 20.3.3. The System Operator shall give a Participant a 30-day advance notice of its intention to impose such financial penalty in order to allow the Participant to argue its case before the System Operator.



#### 20.4. Waiver or discount

- 20.4.1. Consent by Shva and/or the Participant to deviate from the provisions of the Rules in a certain case or a discount and/or postponement granted by Shva and/or the (direct or Represented) Participant to the other party shall not constitute a precedent nor serve to indicate equivalence to another case.
- 20.4.2. Where Shva and/or the (direct or Represented) Participant does not exercise rights under the provisions of the Rules in a certain case, this shall not be deemed as the relaxation or waiver of such rights in another case and such behavior shall not indicate any relaxation or waiver of the rights of Shva and/or the (direct or Represented) Participant under the Rules.

#### 20.5. Notices to System Participants

- 20.5.1. All notices, demands, requests and other messages shall be made in writing and sent by email and/or registered mail according to such contact details as updated in Annex 1 to these Rules.
- 20.5.2. Any such notice shall be deemed to have reached its destination immediately in the case of personal delivery, or, if sent by email – at the lapse of two Business Days, or at the lapse of four Business Days from the day of dispatch by registered mail, or immediately upon receipt of confirmation of arrival when the email is opened (to the extent that such confirmation exists) by the System Participant.

#### 20.6. Issuance of test cards

- 20.6.1. For the issuance of test cards for the performance of tests pertaining to the System operations, the applicant is responsible for applying to “Issuer”-type System Participants.
- 20.6.2. Subject to Bank of Israel instructions, the Issuer is responsible for issuing test cards to EMV Software Manufacturers for the purpose of authorizing Terminals, including a reasonable service time (SLA) for response and receipt of the cards.
- 20.6.3. Below are the contact details and relevant information for ordering test cards (as provided to the System Operator):

	Cal	Max	Isracard
Contact Address	<a href="mailto:tbankim@icc.co.il">tbankim@icc.co.il</a>	<a href="mailto:betty_b@max.co.il">betty_b@max.co.il</a> <a href="mailto:galit_avi@max.co.il">galit_avi@max.co.il</a>	<a href="mailto:lhagebi@isracard.co.il">lhagebi@isracard.co.il</a> <a href="mailto:iwexler@isracard.co.il">iwexler@isracard.co.il</a>
Application transfer requirements	1) Test Card Issuance Application Form 2) Direct Debit Authorization Form	Test Card Issuance Application Form	Application sent by email
SLA	Up to 7 Business Days from the moment of receipt of a full application, including the direct debit authorization	Up to 10 Business Days	No-plastic card – up to 24 hours Plastic card – up to 2 Business Days
Manner of Dispatch	Self-collection from the reception counter at the companies' offices		



<b>Card Validity</b>	<b>One year</b>	<b>One year</b>	<b>Five years</b>
<b>Card Loss</b>	To block the card, write to the contact address. To receive a new card, follow the new card issuance process.	Because a test card is concerned, blocking the card is not necessary. To receive a new card, follow the new card issuance process.	Because a test card is concerned, blocking the card is not necessary. To receive a new card, follow the new card issuance process.
<b>Card Types</b>	Visa Mastercard Diners	Visa – Platinum Mastercard – Platinum PL	Visa Mastercard PL American Express
<b>Number of Cards</b>	Limited, up to 3 cards	Limited, up to 5 cards	No-plastic card – unlimited  Plastic card – Limited, up to 3 cards