Special Conditions for Payments via Debit Card in connection with a Card Account

For the use of the payments enabled by the Solarisbank AG (hereinafter referred to as the "**Bank**") via a physical debit card (hereinafter referred to as the "**Physical Card**") or virtual debit card (hereinafter referred to as the "**Virtual Card**" and together with the Physical Card referred to as the "**Cards**") in connection with a card account and using a partner app or partner website (hereinafter referred to as the "**Partner App**") the following special terms and conditions shall apply in addition to the Bank's General Terms and Conditions, the respective Terms and Conditions for Payments by Direct Debit under the SEPA Core Direct Debit Scheme, the respective Conditions for Online Banking, the respective Terms and Conditions for the Debit Cards (if a Physical Card has been issued), the respective Conditions for Payments via Virtual Debit Cards and any additional special terms and conditions for the use of the respective partners (e.g. Google Pay). In the event of any conflict between these Special Conditions and other terms and conditions, the provisions of these Special Conditions shall prevail. These Special Conditions as well as the other terms and conditions can be viewed, saved in readable form and printed from https://www.solarisbank.com/de/kundeninformation.

I. Range of applications

1. General

(1) The Cards issued by the Bank are debit cards which are provided to the customer for payment transactions. The Cards may be made available as Physical Cards and as Virtual Cards which are provided to the customer exclusively in virtual form for storage on a telecommunications, digital or IT device (mobile terminal). These Special Conditions shall apply equally to both types of Cards, unless expressly stated otherwise.

(2) In order to be able to use a Card for payment purposes, the customer must be a user of the Partner App through which the card account and thus the Card is managed and through which the customer receives messages and statements from the Bank. The Bank is not obliged to enable the use of a Card if the customer is not or no longer a user of the Partner App. In order to be able to use a Card for payment purposes, the validity of the partner's special terms and conditions applicable to the use of the Partner App (hereinafter referred to as the "**Partner Terms and Conditions**") must be validly agreed between the customer and the partner.

2. Applications of the Virtual Card related to payment transactions

The customer may use the Virtual Cards for payment at all point-of-sale terminals with VISA contactless acceptance both in Germany and, as an additional service, abroad.

3. Applications of the Physical Card

3.1 For payment transactions

(1) The customer may use the Physical Card in Germany and, as an additional service, abroad within the network of the respective payment card association (e.g. Visa or Mastercard) for payments at contracting companies on site at automated cash registers and online.

(2) The contracting companies and the financial institutions can be identified by the acceptance symbols that also appear on the Physical Card. If the Physical Card is associated with additional services (e.g. assistance in emergencies, insurance policies), these are governed by the applicable special provisions.

3.2 As a storage medium for additional applications

If the Physical Card issued to the customer has a chip, the Physical Card may be used as a storage medium for additional applications

- of the Bank that issues the Physical Card in accordance with the contract concluded with the Bank (bank-generated additional application); or
- of a contracting company in accordance with the contract concluded with the latter (company-generated additional application).

4. Personal identification number (PIN) for the Physical Card

(1) The customer shall be provided with a personal identification number (PIN) for use at automated checkouts with his/her Physical Card.

(2) If the PIN is entered incorrectly three times in succession, the Physical Card can no longer be used at automated checkouts in which the PIN must be entered to use the Physical Card. In this case, the customer should contact the partner of the Bank who provides the user interface.

II. Card functions and types of use

The Bank agrees with each customer which of the following card functions of the Card can be used by the customer in addition to the linked card account and reference account.

1. Card Account linked to the Card

(1) For the purpose of using the Card, the Bank shall maintain a settlement account (hereinafter referred to as the "**Card Account**") for the customer for all card functions in accordance with Section II, Clauses 3 and 4 of these Special Conditions. The Card Account shall be maintained in the name of the customer. An IBAN shall be assigned to the account.

(2) The Card Account is used for processing payments with the Card. The customer may not use the Card Account for SEPA direct debits. The Bank rejects all incoming SEPA direct debits without exception and charges a fee for rejecting the direct debit (see the Bank's "List of Prices and Services" for the fee due).

(3) Refunds (e.g. from contracting companies) are credited to the Card Account.

(4) Credit balances on the Card Account may only be paid out in form of transfers to the reference account, provided that such credit balance has not been used otherwise through previously authorised disposals.

2. Reference account

(1) The customer shall specify to the Bank at least one account with regular incoming payments (e.g. salary account) that supports SEPA direct debits, is in the customer's name and has an IBAN in the customer's country of residence (hereinafter referred to as the "**Reference Account**").

(2) Customers to whom the Bank has granted the card function in ac-

cordance with Section II, Clause 4 of these Special Conditions undertake to provide the Bank with a SEPA direct debit mandate for the Reference Account for the purpose of settling a negative balance on the Card Account.

(3) The Bank will validate the Reference Account by means of a so-called Digital Account Snapshot. This will be done by the partner's inspection of the customer's Reference Account, provided the partner is allowed to provide account information services, or by external service providers commissioned by the Bank (FinLeap Connect, FinTecSystems).

(4) The customer can change the Reference Account in the Partner App. If the customer changes the Reference Account, he/she is obliged to provide the Bank with a new SEPA direct debit mandate for this account. The Bank shall validate the IBAN of the new Reference Account as described in Section II, Clause 2 paragraph 3 of these Special Conditions.

3. Pre-paid function

(1) The customer can top up his/her Card Account by means of transfer.

(2) The customer can make payments using the pre-paid function, provided his/her Card Account has a positive balance. The customer can use the topped-up credit for payments with the Card.

4. Card with credit limit

4.1. Limit

(1) In addition to the pre-paid function of the Card in accordance with Section II, Clause 3 of these Special Conditions, the Bank grants the customer a maximum limit of EUR 1,000 (hereinafter referred to as the "**Limit**"). An increase of this Limit beyond this amount during the business relationship is possible and will be communicated to the customer separately through a message in the Partner App.

(2) Within this Limit, the customer may carry out transactions with the Card which may result in a maximum negative balance of the Card Account in the amount of the Limit.

(3) The Bank shall determine the customer's Limit at its reasonable discretion and taking into account, inter alia, the customer's creditworthiness and shall inform the customer separately of the respective Limit.

(4) The Limit of the customer is checked by the Bank on a regular basis. The Bank is entitled, at its reasonable discretion, in the event that the SCHUFA rating of the customer falls below SCHUFA rating level G, in the event of suspected unauthorised or fraudulent use of the Card, in the event of Non-Payment pursuant to Section IV, Clause 1.2 of these Special Conditions, in the event of rejection of another SEPA direct debit to the Reference Account, or in the event of a substantial deterioration in the customer's financial circumstances that occurs or threatens to occur and thereby jeopardises the fulfilment of any other obligation vis-à-vis the Bank, to reduce the Limit to zero and to authorise the Card only for payments within the scope of the pre-paid function. Depending on the customer's creditworthiness, the Bank may, at its reasonable discretion, again set a Limit within the credit limit provided for in paragraph 1. The Bank shall notify the customer separately of the respective Limit.

4.2 Settlement of negative balances

(1) Negative balances on the Card Account which are within the respective Limit agreed upon shall bear interest of 0% for the customer.

(2) After a payment with the Card, the customer is obliged to settle any negative balance on the Card Account resulting from such payment.

(3) The Bank shall, by means of the SEPA direct debit mandate provided to it, debit the corresponding amount pursuant to paragraph 2 from the specified Reference Account to settle the negative balance on the Card Account. All payments shall be debited from the Reference Account individually by SEPA direct debit or combined into one SEPA direct debit per day. The customer will be notified of the SEPA direct debit and the amount to be debited two days before the SEPA direct debit is executed by means of a push message or by a message in the Partner App.

4.3. Rejection of the direct debit

If a SEPA direct debit to the Reference Account is rejected, the Bank will debit the Card Account with a fee according to the Bank's "List of Prices and Services". The Bank shall inform the customer without undue delay (*unverzüglich*) of a SEPA direct debit that has been rejected.

4.4 Default of the customer in case of non-payment

(1) In the event of non-payment of the amount owed pursuant to Section II, Clause 4.2 paragraph 2 of these Special Conditions within 4 days of the respective payment with the Card, the customer shall be in default without further notice.

(2) If the customer is in default, the Bank is entitled to charge default interest at the statutory rate in accordance with Section 288 paragraph 1 BGB.

(3) The Bank retains the right to provide evidence of further damage; the customer remains the right to provide evidence of no or less damage.

(4) The customer may settle a negative balance on the Card Account by transferring a corresponding amount from the Reference Account. If this results in a credit balance on the Card Account, the provisions relating to the pre-paid function shall apply in accordance with Section II, Clause 3 of these Special Conditions.

III. Authorisation of payments

1. Authorisation of payments with the Virtual Card

(1) When using the Virtual Cards at point-of-sale terminals, each payment transaction must be approved by means of biometric features (fingerprint scan or facial recognition) or the unlock code of the device (password) (authentication elements), unless this is exceptionally waived due to the type of payment, e.g. for small amounts.

(2) When using Virtual Cards in online commerce, the customer may, after prior consultation between the customer and the contracting company, exceptionally waive the requirement to sign a receipt and instead only provide the Virtual Card number.

(3) In online commerce, the authentication of the customer can also be made by using the separately agreed authentication elements on request. Authentication elements are

- Knowledge elements (something the customer knows, e.g. an online password);
- possession elements (something that the customer possesses, e.g. a mobile device for generating and receiving one-time usable transaction numbers (TAN) as proof of possession); or
- being elements (something that is the customer, e.g. fingerprint).

(4) By using the Virtual Cards at point-of-sale terminals or in online commerce in accordance with paragraphs 1 to 3 and the release in accordance with paragraph 1 or paragraph 3 (if required), the customer is giving consent (authorisation) to complete the payment. Once consent has been given, the customer cannot cancel the payment.

2. Authorisation of payments with the Physical Card

(1) When using the Physical Card, either

- a receipt on which the contracting company has entered the Physical Card details must be signed, or
- the PIN must be entered at automated checkouts.

After prior consultation between the customer and the contracting company, the customer may exceptionally refrain from signing the receipt - in particular to speed up a business transaction within the framework of a telephone contact - and instead merely state his/her Physical Card number.

When the Physical Card is used at automated cash registers, it is not necessary to enter the PIN:

- For payment of traffic usage fees or parking fees at unattended automated checkouts.
- For contactless payment of small amounts. The Physical Card with contactless function must be held against a card reader. The amount and financial usage limits specified by the Bank apply.

For online payments, the customer is authenticated by using the separately agreed authentication elements on request. Authentication elements are

- Knowledge elements (something the customer knows, for example, an online password);
- Possession elements (something that the customer possesses, for example, mobile device for the generation of a onetime usable transaction numbers (TAN) as proof of possession); or
- Being elements (something that is the customer, for example fingerprint).

(2) By using the Physical Card, the customer is giving consent (authorisation) to complete the card payment. If, in addition, a PIN or signature is required for this, consent is given only when this is provided. Once consent has been given, the customer cannot cancel the card payment. The authorisation also includes the express consent that the Bank processes, transmits and stores the personal data of the customer which is necessary for the execution of the card payment.

IV. Execution modalities

1. Blocking of an available amount of money

1.1 General

The Bank shall be entitled to block an amount of money available on the Card Account within the limits of the financial usage limit (cf. Section IV, Clause 4 of these Special Conditions) if

- the payment transaction has been triggered by the payee, and
- the customer also agrees to the exact amount of the amount of money to be blocked.

Without prejudice to any other legal or contractual rights, the Bank shall release the exact amount of money without undue delay (*unverzüglich*) after having been notified of the exact payment amount or after the payment order has been received.

1.2 Card with credit limit – Non-payment; blocking in case of non-payment

If the customer does not settle a negative balance despite the Bank's notification of the corresponding SEPA direct debit in accordance with Section II, Clause 4.2, paragraph 3 of these Special Conditions (hereinafter referred to as the "**Non-Payment**"), the Bank may block the relevant Card for further payments. The Bank shall unblock the Card after the negative balance has been settled (Section VII, Clause 5 paragraph 3 of these Special Conditions).

2. Rejection of payments by the Bank

The Bank is entitled to reject the payment if

- the customer - in case of a Physical Card - has not confirmed it with his/her PIN or - in case of the Virtual Card or the Physical Card - has not confirmed it with biometric features, an online password or the entry of a password code on the mobile device,
- the financial usage limit has not been observed, or
- the respective Card is blocked.

The customer will be informed of this via the terminal at which the Card was used or via the respective Partner App.

3. Completion period

The payment process is triggered by the payee. On receipt of the payment order by the Bank, the latter is obliged to ensure that the payment amount is received by the payee's payment service provider at the latest by the time specified in the "List of Prices and Services".

4. Financial usage limit

The customer may only use the respective Card within the credit balance on the respective Card Account or within the Limit.

Even if the customer does not comply with the financial usage limit, the Bank is entitled to demand reimbursement of the expenses that arise from the use of the Card. The approval of individual transactions does not entail either the provision of credit or an increase of a credit amount previously agreed, but is given in the expectation that the settlement of the transactions is guaranteed when they become due.

If the booking of the transactions exceeds the existing account balance or a Limit previously agreed, the booking shall lead to a tolerated overdraft.

The debit interest for the tolerated overdraft is set out in the Bank's "List of Prices and Services".

V. Declarations and account statements

1. Retrieval of documents

(1) Within the framework of the business relationship between the Bank and the customer, the Bank and the customer agree that the Card Account and thus the Card will be managed through the Partner App. The Bank will send notifications regarding the use of the Card Account and the Card, including account statements, periodic balance statements, payment reminders, dunning notices and SEPA direct debit notifications, to the customer via the Partner App or by e-mail.

(2) Accordingly, the Bank and the customer agree that, in addition to communication by e-mail, the Partner App is the customer's device for receiving all communications and declarations of the Bank, in particular account statements and periodic balance statements.

2. Notifications

(1) Unless the written form has been expressly agreed with the customer or is required by law, notices and declarations of the Bank are provided to the customer in electronic form by e-mail or via the Partner App.

(2) In accordance with these Special Conditions, the customer expressly waives the right to receive notifications communicated by e-mail or via Partner App by post. The Bank fulfils its obligation to transmit, inform of or otherwise make available the relevant notifications by sending them by e-mail or posting them on the Partner App.

(3) Notwithstanding the foregoing, the Bank shall, in addition to the provision of notifications and declarations via the Partner App, be entitled to send such notifications and declarations by post if this is necessary for legal reasons or expedient for other reasons (e.g. the temporary outage of the Partner App). The expenses for postal dispatch shall be reimbursed to the Bank in accordance with the Bank's List of Prices and Services.

3. Cooperation obligations

(1) The customer is obliged to regularly and promptly, but at least once a month, retrieve notifications and declarations via the Partner App and to review the respective contents.

(2) The customer shall check the notifications for completeness and correctness.

(3) Any discrepancies shall be reported to the Bank without undue delay (*unverzüglich*), at the latest, however, six weeks after being made available via the Partner App.

4. Receipt

All notifications and declarations sent to the customer by e-mail or via the Partner App are deemed to have been received when the e-mail is sent or when the Bank informs the customer about the posting and the possibility of retrieval via the Partner App.

VI. Customer's duty of care and cooperation obligations

1. General customer's duty of care and cooperation obligations

1.1 Protection of the authentication elements for payment transactions

The customer shall take all reasonable precautions to protect his/her authentication elements for payment transactions agreed with the Bank (cf. Section III, Clause 1 paragraph 1 of these Special Conditions for the Virtual Card and Section III, Clause 2 paragraph 1 of these Special Conditions for the Physical Card) from unauthorised access. Otherwise, there is a risk that the authentication elements for payment transactions may be misused or used otherwise not authorised.

In order to protect the individual authentication elements for payment transactions, the customer shall pay particular attention to the following:

(a) Knowledge elements, such as the password, shall be kept secret; they may in particular

- not be communicated orally (e.g. by telephone or in person),
- not be passed on outside of payment transactions in text form (e.g. by e-mail or messenger service);
- not be stored unsecured electronically (e.g. storage of the password in plain text on the mobile device); and
- not be recorded on a device or stored as a transcript together with a device which serves as a possession element (e.g. mobile device) or for checking the being element (e.g. mobile device with application for payment and fingerprint sensor).

(b) Possession elements, such as a mobile device, shall be protected from misuse, in particular

- it must be ensured that unauthorised persons cannot access the customer's mobile device (e.g. mobile telephone);
- it must be ensured that other persons cannot use the Partner App on the mobile device (e.g. mobile telephone);
- the Partner App on the mobile device of the subscriber must be deactivated before the subscriber gives up possession of this mobile device (e.g. by selling or disposing of the mobile phone); and
- the proofs of possession (e.g. TAN) may not be passed on orally (e.g. by telephone) or in text form (e.g. by e-mail, messenger service) outside the online payment processes.

(c) Being elements, such as the customers fingerprint, may only be used as an authentication element on a mobile terminal of the customer for payment transactions if no other person's being elements are stored on the mobile device. If the mobile device used for payment transactions stores the identity elements of other persons, the knowledge element issued by the Bank (e.g. online password) is to be used for online payment transactions and not the identity element stored on the mobile device.

1.2 Control obligations for online payment transactions

If, in the case of payment transactions, the customer is notified of details of the payment transaction (e.g. the name of the contracting company and the amount of the transaction), the customer shall check this data for correctness.

2. Specific customer's duty of care and cooperation obligations for the Physical Card

2.1 Signature

Upon receipt of his/her Card, the customer shall sign the signature strip immediately.

2.2 Safekeeping of the Card

The Physical Card must be kept safe with particular care in order to prevent it from being lost or misused. In particular, it must not be kept unattended in a vehicle. Anyone who is in possession of the Physical Card is able to use it for improper transactions.

2.3 Confidentiality of the PIN

The customer shall ensure that no one else gains knowledge of his/her PIN. In particular, it must not be written on the Physical Card or otherwise kept with it. Anyone who gains knowledge of the PIN and comes into possession of the Physical Card is able to use the PIN and the Physical Card for improper transactions.

3. Customer's notification and reporting obligations

(1) If the customer becomes aware of the loss or theft of his/her Physical Card, the improper use of his/her Virtual Card or Physical Card or any other unauthorised use of the Virtual Card or Physical Card or the PIN, the Bank or a representative office of the payment card association (e.g. Visa or Mastercard) shall be notified immediately to arrange for the respective Card to be blocked. The customer shall report any theft or misuse to the police without undue delay (*unverzüglich*).

(2) The customer shall notify the Bank without undue delay (*unverzüglich*) after having identified an unauthorised or incorrectly executed transaction.

4. Specific customer's notification and reporting obligations for the Physical Card

(1) If the customer suspects that someone else has come into possession of his/her Physical Card illegitimately, it is being used improperly or any other unauthorised use of the Physical Card or PIN is being made, he/she shall also submit a blocking notification without undue delay (*unverzüglich*).

(2) If the Physical Card has a TAN generator or a signature function, blocking the Physical Card also results in blocking access to online banking.

(3) Blocking of a company-generated additional application can only be carried out by the company that has saved the additional application to the chip on the Physical Card and is only possible if the company has provided the option to block its additional application. Blocking of a bank-generated additional application can only be carried out by the card-issuing Bank and is governed by the contract concluded with the card-issuing Bank.

VII. Payment obligations

1. Payment obligation of the customer

The Bank is obliged to the respective contracting company to settle the transactions made by the customer with the Card.

Objections and other complaints by the customer arising from the contractual relationship with a contracting company with which the Card was used shall be pursued directly with that contracting company.

2. Foreign currency conversion

(1) If the customer uses the Card for transactions that are not in euros, the Card Account shall still be charged in euros.

(2) The exchange rate for foreign currency transactions shall be determined on the basis of the Bank's "List of Prices and Services".

(3) A change to the reference exchange rate specified in the conversion regulation shall take effect immediately and without prior notification of the customer.

3. Fees

(1) The fees owed by the customer to the Bank shall be determined on the basis of the Bank's "List of Prices and Services".

(2) Changes to the fees shall be proposed to the customer in written form no later than two months before they are to take effect. If the customer has agreed to an electronic means of communication with the Bank as part of the business relationship, the changes may also be proposed by this means. The customer may either agree or reject the changes before the proposed date of entry into force. The customer is deemed to have consented if he/she fails to provide notice of his/her rejection in advance of the proposed date of the changes coming into effect. The Bank shall make specific reference to this de facto consent in its offer.

(3) When the customer is notified of changes to the fees, he/she may terminate the business relationship without notice and at no cost in advance of the proposed date of the changes coming into effect. The Bank shall make specific reference to this right to terminate in its offer.

4. Customer's entitlement to reimbursement, revision and compensation

4.1 Reimbursement in case of unauthorised transaction

In case of an unauthorised transaction in the form of use of the Card with a contracting company, the Bank does not have any claims against the customer for reimbursement of its expenses. The Bank is obliged to reimburse the customer the amount in full and without delay (*unverzüglich*). If the amount has been debited from an account, the Bank shall restore it to the balance that it would have had if the unauthorised transaction using the Card had not taken place. This obligation must be fulfilled no later than the end of the business day following the day on which the Bank was notified that the transfer is unauthorised or has otherwise learned thereof. If the Bank has informed a competent authority in writing of justified grounds for suspecting fraudulent conduct on the part of the customer, the Bank must examine its obligation under sentence 2 without undue delay (*unverzüglich*) and fulfil this obligation when the suspicion of fraud is not confirmed.

4.2 Claims for non-execution, incorrect or belated execution of an authorised transaction

(1) In case of non-executed, belated or incorrect processing of an authorised transaction in the form of use of the Card with a contracting company, the customer may demand from the Bank the immediate and full reimbursement of the transaction amount insofar as the transaction failed to take place or was incorrect. If the amount has been debited from an account, the Bank shall restore it to the balance that it would have had if the failed or incorrect transaction had not taken place.

(2) In addition to paragraph 1, the customer may demand reimbursement by the Bank of any fees or interest that were charged to him/her or debited from his/her account in connection with the authorised transaction that failed to take place or was processed incorrectly.

(3) If the payment amount is received by the payee's payment service provider only after expiry of the execution period specified under Section IV, Clause 3 of these Special Conditions, the payee may require his/her payment service provider to credit the payment amount to the payee's account as if the card payment had been duly executed.

(4) If an authorised transaction failed to take place or was processed incorrectly, the Bank shall at the request of the customer investigate the transaction and report the findings to him/her.

4.3 Compensation entitlements by the customer on the basis of an unauthorised transaction or non-executed or incorrect processing of an authorised transaction

In the case of an unauthorised transaction or in the case of a non-executed, belated or incorrect processing of an authorised transaction, the costumer may demand compensation from the Bank for losses not already covered under Section VII, Clause 4.1 and 4.2 of these Special Conditions. This does not apply if the Bank was not responsible for the breach of obligation. In this context, the Bank is responsible for obligations incurred by an intermediary that it has appointed as if they had been incurred by the Bank itself, unless the main cause was the responsibility of an intermediary specified by the costumer. If the Card is used in a country outside Germany and the European Economic Area, the liability of the Bank for the culpability of a body involved in processing the payment transaction is restricted to the careful selection and instruction of such a body. If the costumer has contributed to the occurrence of a loss through culpable conduct, the principles of contributory culpability shall determine the extent to which the Bank and the customer shall bear the loss. Liability under this paragraph is limited to EUR 12,500 per transaction. This limitation to the amount of liability does not apply

- for transactions not authorised by the customer using the Card;
- in the event of malicious intent or gross negligence on the part of the Bank;
- to risks that the Bank has specifically taken on; and
- to losses of interest incurred by the costumer.

4.4 Period for pursuit of claims under Section VII, Clauses 4.1 to 4.3

Claims against the Bank in Section VII, Clauses 4.1 to 4.1 of these Special Conditions are excluded if the costumer has not notified the Bank that a transaction is unauthorised, has not been completed, is belated or is incorrect at the latest 13 months from the date on which the transaction was charged. The 13-month notification period commences only when the Bank has notified the costumer of booking of the charge resulting from the transaction by the agreed means, at the latest within a month of booking of that charge; otherwise, the day of such notification shall determine commencement of the period. Claims for liability under Section VII, Clause 4.3 of these Special Conditions may still be pursued by the costumer after expiry of the notice period under sentence 1 if he/she was unable to meet the deadline for reasons beyond his/her control.

4.5 Claim for reimbursement in the event of an authorised transaction without a specific amount and period for pursuit of the claim

(1) The costumer may demand full reimbursement of the transaction amount without undue delay (*unverzüglich*) if he/she has authorised a transaction with a contracting company in such a way that

- the exact amount was not specified on authorisation; and
- the payment process exceeds the amount that the costumer could have expected given his/her previous spending behaviour, the content of the card contract and the relevant circumstances of the individual case; reasons related to any currency conversion cannot be considered if the agreed reference exchange rate was used as the basis.

(2) The costumer is obliged to explain the circumstances on which the claim for reimbursement is based to the Bank.

(3) The claim for reimbursement is excluded if it has not been pursued with the Bank within eight weeks of the date on which the transaction was charged to the Reference Account.

4.6 Exclusion of liability and objection

Claims of the costumer against the Bank under Section VII, Clauses 4.1 to 4.5 of these Special Conditions are excluded if the circumstances on which a claim is based

- result from on an unusual and unforeseeable event over which the Bank has no influence, and the consequences of which could not have been avoided despite exercising reasonable care (*gebotenen Sorgfalt*); or
- are brought about by the Bank as the result of a statutory obligation.

5. Liability of the costumer for unauthorised transactions

5.1 Liability of the costumer until the blocking notification when using the Virtual Card

(1) If the Virtual Cards is misused and this results in unauthorised transactions in the form of use of the Virtual Cards with a contracting company, the customer shall only be liable for damage caused up to the time of the blocking notification up to a maximum of EUR 50, irrespective of whether the customer is to blame for the loss, theft or other loss or other misuse.

(2) The customer shall not be liable in accordance with paragraph 1 if it has not been possible for him/her to notice the misuse of the respective Virtual Card before unauthorised access.

(3) If unauthorised transactions are made prior to the blocking notification and if the customer has acted fraudulently or has violated his/her duties of care under these Special Conditions intentionally (*vorsätzlich*) or with gross negligence (*grob fahrlässig*), the customer shall bear the full extent of the resulting damage. Gross negligence (*grobe Fahrlässigkeit*) on the part of the customer may be deemed to have occurred in particular if the customer culpably (*schuldhaft*) failed to notify the Bank or a representative office of the payment card association (e.g. Visa or Mastercard) of the loss or the theft or the misuse of the transaction without undue delay (*unverzüglich*) after becoming aware of it.

5.2 Liability of the costumer until the blocking notification when using the Physical Card

(1) If the customer misplaces his/her Physical Card or PIN, they are stolen from him/her or lost or the Physical Card or the authentication instruments agreed for online payment transactions are otherwise misused and, as a result, unauthorised card transactions are carried out in the form of use of the Physical Card with a contracting company, the customer is liable for losses incurred up to the blocking notification, up to a maximum of EUR 50, irrespective of whether the customer is to blame for the loss, theft or other loss or other misuse.

(2) The customer shall not be liable in accordance with paragraph 1 if

- it has not been possible for him/her to notice the deprivation, theft, loss or any other misuse of the Physical Card prior to the unauthorised payment process, or
- the loss of the Physical Card has been caused by an employee, an agent, a branch of a payment service provider or a body to which the Bank's activities have been outsourced.

(3) If unauthorised transactions are carried out before the blocking notification and the customer has acted with fraudulent intent or breached his/her duty of care as specified in these Special Conditions intentionally or as a result of gross negligence, the customer is responsible for the resulting losses in full. Gross negligence of the customer may exist, in particular, if

- he/she has culpably failed to notify the Bank or a representative office of the payment card association (e.g. Visa or Mastercard) immediately after he/she becomes aware of the loss, theft or improper use of the Physical Card,
- the personal identification number or the agreed knowledge element for online payment transactions (e.g. online password) has been written on the Physical Card or has been kept with the Physical Card (e.g. in the form of the original letter in which it was communicated to the customer),
- the personal identification number or the agreed knowledge element for online payment transactions (e.g. online password) has been communicated to another person and the misuse has resulted from this.

5.3 General provisions on the customer's liability until the blocking notification

(1) If the Card is used in a country outside Germany and the European Economic Area, the customer shall bear the loss pursuant to Section VII, Clause 5.1 paragraph 1 and Clause 5.2 paragraph 1 of these

Special Conditions in excess of a maximum of EUR 50, if the customer has negligently breached the obligations incumbent upon him/her under these Special Conditions. If the Bank has contributed to the occurrence of the loss through a breach of its obligations, the Bank shall be liable for the loss incurred to the extent of the contributory negligence for which it is responsible.

(2) Liability for losses caused within the period for which the transaction limit applies is limited in each case to the respective Limit or - In case of a pre-paid Card in accordance with Section II, Clause 3 of these Special Conditions - the respective balance on the Card Account.

(3) The customer is not obliged to compensate for the loss pursuant to paragraphs 1 and 2 if the customer was unable to submit the blocking notification because the Bank had not secured the possibility of accepting the blocking notice.

(4) In deviation from paragraphs 1 and 2, the customer shall not be obliged to pay compensation if the Bank has not required the customer to provide strong customer authentication within the meaning of Section 1 paragraph 24 of the Payment Services Supervision Act (*Zahlungsdiensteaufsichtsgesetz*, *ZAG*) or if the payee or his/her payment service provider has not accepted such strong customer authentication although the Bank was obliged to provide strong customer authentication pursuant to Section 55 ZAG. Strong customer authentication requires in particular the use of two independent authentication elements from the categories of knowledge (e.g. the password), possession (e.g. the mobile device) or inherence (something that is the customer, e.g. the customer's ”fingerprint”).

(5) Paragraphs 2 to 4 shall not apply if the costumer has acted with fraudulent intent.

6. Liability of the costumer after the blocking notification

As soon as the loss or theft of the Physical Card, the improper use or any other unauthorised use of the Virtual Card, the Physical Card, the PIN or personalised security feature has been reported to the Bank or a representative office of the payment card association (e.g. Visa or Mastercard) by the customer, the Bank is responsible for all subsequent losses in the form of use of the Card with a contracting company.If the customer acts with fraudulent intent, the customer is also responsible for losses incurred after the blocking notification.

7. Ownership and validity of the Physical Card

(1) The Physical Card shall remain the property of the Bank. It is non-transferable. The Physical Card is valid only for the period specified on the Physical Card.

(2) The Bank is entitled to demand return of the old Physical Card when a new Physical Card is issued, at the latest on expiry of its validity. If the right to use the Physical Card ends before this (e.g. by termination of the Physical Card contract), the customer shall return the Physical Card to the Bank without undue delay (*unverzüglich*). The customer shall arrange for additional company-generated applications on the Physical Card to be removed without undue delay (*unverzüglich*) by the company that set up the additional application on the Physical Card. The option to continue using a bank-generated additional application is governed by the contractual relationship between the customer and the card-issuing Bank.

(3) The Bank reserves the right to replace a Physical Card with a new one even during the period of validity of the Physical Card. The customer shall not incur any costs as a result.

(4) When a new Physical Card is issued, the Bank will via the respective payment card association (e.g. Visa or Mastercard) automatically update the relevant payment data (customer name, expiry date and Physical Card number) at contracting parties who also participate in the service. The customer can object to an automatic transmission of the Physical Card data by sending an e-mail to support@solarisbank.de.

VIII. Termination

1. Costumer's right of termination

(1) The costumer may terminate the card contract at any time without any notice period.

(2) Upon termination of the Partner App and/or the Partner Terms and Conditions (Section I, Clause 1, paragraph 2 of these Special Conditions) by the customer, the customer automatically terminates the card contract in accordance with Section VIII, Clause 1 paragraph 1 of these Special Conditions.

2. Right of termination of the Bank

(1) The Bank may terminate the card contract with an appropriate period of notice of at least two months. The Bank shall terminate the card contract with a longer notice period if this is necessary in view of the legitimate interests of the customer.

(2) The Bank may terminate the card contract after twelve (12) consecutive months of inactivity of the customer regarding the Card Account with a two-month notice period.

(3) Without prejudice to the right of termination for good cause pursuant to Section VIII, Clause 2 paragraph 4 of these Special Conditions, upon termination of the Partner App and/or the Partner Terms and Conditions by the partner, the Bank automatically terminates the card contract with a two-month notice period. Upon termination of the Partner App and/or the Partner Terms and Conditions by the partner, the Card shall be blocked for further payments.

(4) The Bank may terminate the card contract without notice if there is good cause (*wichtiger Grund*) which makes it unreasonable for the Bank to continue the card contract, even after due consideration of the legitimate interests of the customer. Such a reason exists, in particular, in case of Non-Payment according to Section IV, Clause 1.2 of these Special Conditions.

3. Consequences of termination

(1) When termination comes into effect, the Card may not be used further.

(2) Any positive balance remaining on the Card Account linked to the Card at the time of termination shall be refunded to the customer at the end of the contractual period, provided that the positive balance is not blocked by an already authorised transaction. The refund shall be made to the Reference Account.

(3) The customer is still required to settle the negative balance without undue delay (*unverzüglich*).

4. Further consequences of termination when using the Physical Card

The Physical Card shall be returned to the Bank without undue delay

(*unverzüglich*) and without request. The customer shall arrange for additional company-generated applications on the Physical Card to be removed without undue delay (*unverzüglich*) by the company that set up the additional application on the Physical Card. The option to continue using a bank-generated additional application is governed by the regulations that apply to the additional application in question.

5. Blocking of the Card

(1) The Bank may block the Card and - in case of a Physical Card - revoke the Physical Card

- if it is entitled to terminate the card contract for good cause (*wichtiger Grund*),
- in case of Non-Payment pursuant to Section IV, Clause 1.2 of these Special Conditions,
- if material grounds in connection with the security of the Card justify it, or
- if there is a suspicion of unauthorised or fraudulent use of the Card.

(2) The Bank shall notify the customer of the block, specifying the relevant reasons, if possible before the block, but at the latest immediately after the block.

(3) If the Card was blocked due to Non-Payment pursuant to Section IV, Clause 1.2 of these Special Conditions, the Bank will unblock the Card after the negative balance has been settled. If the Card has been blocked for another reason, the Bank will unblock the Card at the customer's request and, in the case of a Physical Card, replace it with a new Physical Card once the reasons for blocking cease to exist. The Bank shall also inform the customer of an unblocking in accordance with this paragraph without undue delay (*unverzüglich*).

6. Additional provisions for Physical Cards

(1) If the Physical Card has a TAN generator or a signature function for online banking, blocking the Physical Card also results in blocking access to online banking.

(2) If the customer has saved an additional application on a revoked Physical Card, revocation of the Physical Card means that he/she can no longer use the additional application. The customer may demand from the Bank release of company-generated additional applications stored on the Physical Card at the time of its revocation, once the latter has received the Physical Card from the place at which it was revoked. The Bank is entitled to fulfil the demand for release of company-generated additional applications by providing the customer with the Physical Card with the payment functions removed from it. The option to continue using a bank-generated additional application on the Physical Card is governed by the regulations that apply to the additional application in question.

IX. Additional applications

1. Saving additional applications on the Physical Card

(1) The chip on the Physical Card can also be used as a storage medium for a bank-generated additional application (e.g. in the form of a feature for protection of minors) or for a company-generated additional application (e.g. in the form of an electronic travel ticket).

(2) The use of a bank-generated additional application is determined by the legal relationship of the customer to the card-issuing Bank.

(3) The customer may use a company-generated additional application in accordance with the terms of the contract concluded with the company. The customer shall decide whether he/she wishes to use his/her Physical Card to save a company-generated additional application. A company-generated additional application is saved to the Physical Card at the company's terminal by agreement between the customer and the company. Financial institutions are not aware of the content of the data communicated at the company's terminal.

2. Responsibility of the company for the content of a company-generated additional application

The card-issuing Bank only provides the technical platform, in the form of the chip on the Physical Card, that allows the customer to save company-generated additional applications to the Physical Card. Any service that the company provides for the customer via the company-generated additional application is governed exclusively by the content of the contractual relationship between the customer and the company.

3. Processing of complaints with additional applications

(1) The customer shall pursue objections relating to the content of a company-generated additional application exclusively with the company that saved the additional application to the Physical Card. The company shall process such objections on the basis of the data stored with it. The customer may not hand over the Physical Card to the company for the purposes of processing the complaint.

(2) The customer shall pursue objections relating to the content of a bank-generated additional application exclusively with the Bank.

4. No information about the PIN issued to the customers by the Bank in company-generated additional applications

When saving, making changes to the content of or using a company-generated additional application on the Physical Card, the PIN issued to the customer by the card-issuing Bank shall not be entered.

If the company that has saved a company-generated additional application to the Physical Card gives the customer the opportunity to secure access to this additional application with a separate legitimation medium selected by him/her, the customer may not use the PIN that has been given to him/her by the card-issuing Bank for use of the payment transaction applications to safeguard the company-generated additional application.

5. Blocking options for additional applications

Blocking of a company-generated additional application can only be carried out by the company that saved the additional application to the chip on the Physical Card and is possible only if the company has provided the option to block its additional application. Blocking of a bank-generated additional application can only be carried out by the Bank and is governed by the contract concluded with the Bank.