

Terms and Conditions for the MasterCard (credit card)



I Payment-related card functions

1 Card facilities

1.1 For payments

The MasterCard is a credit card. The MasterCard issued by the Bank can be used by the cardholder both in Germany and, as an additional service, abroad at any MasterCard outlet

- for payment at contractual partners using automated cash registers or online, and
- as an additional service, to withdraw cash both from cash dispensers (ATMs) and, on presentation of appropriate identification documents, also from financial institutions (cash service).

The contractual partners as well as the financial institutions and cash dispensers that participate in the cash service can be identified by the acceptance symbols displayed on the MasterCard. If the MasterCard offers additional services (e.g. assistance in emergencies, insurance), such services shall be governed by the special terms and conditions applicable to such services.

The card can be issued as a physical card or as a digital card for storage on a telecommunications, digital or IT device (mobile terminal). These conditions apply to both types of card, unless expressly stated otherwise. For the digital card, the terms of use for the digital card agreed separately with the Bank shall also apply.

1.2 As a storage medium for additional applications

If the MasterCard issued to the cardholder has a chip, it can also be used as a storage medium for additional applications

- of the card-issuing Bank in accordance with the agreement concluded with the Bank (additional Bank-generated applications), or
- of a contractual partner in accordance with the agreement concluded with that partner (additional company-generated applications).

2 Personal identification number (PIN)

To use electronic cash terminals at contractual partners and cash dispensers, the cardholder can be provided with a personal identification number (PIN) for his/her card. The card may no longer be used at electronic cash terminals or cash dispensers, where the PIN has to be entered in combination with the card, once an incorrect PIN has been entered three times in succession. If this has occurred, the cardholder should contact his/her Bank, if possible the account holding branch.

3 Authorisation of card payments by the cardholder

(1) When using the MasterCard, the cardholder must

- sign a sales slip to which the contractual partner has added the card data, or
- enter the PIN at cash dispensers and electronic cash terminals.

By prior agreement between the cardholder and the contractual partner, the cardholder may in exceptional circumstances – particularly to speed up a transaction conducted by telephone – omit to sign the sales slip and instead merely inform the company of his/her MasterCard number.

In the case of payment at automated tills, it is not necessary to enter the PIN:

- for payment of traffic fees or parking fees at unattended automated cash registers.
- for contactless payment of small amounts. The MasterCard with contactless function must be held against a card reader. The amount and usage limits set by the bank apply.

For online payments, the cardholder shall be authenticated by using the separately agreed authentication elements upon request. Authentication elements are derived from the cardholder's

- knowledge (something the cardholder knows, for example, an online password),
- possession (something that the cardholder owns, for example, a mobile terminal for generating a one-time usable transaction number [TAN] as proof of ownership) or
- inherence (something that the cardholder is, e.g. fingerprint).

(2) By using the card, the cardholder authorises the execution of the card payment. If a signature, PIN or other authentication element is also required, the payment is only authorised once the PIN has been entered or the signature given. Once the cardholder has authorised a card payment, he/she can no longer revoke it. This authorisation also includes the express consent that the Bank may process, transmit and store the personal data of the cardholder necessary for the execution of the card payment.

4 Blocking an available credit balance

The Bank shall be entitled to block an available credit balance on the cardholder's account within the limits of the financial limit of use (see Section I.7), if

- the payment transaction has been triggered by or via the payee and



- the cardholder also agrees to the exact amount of money to be blocked.

The Bank shall release the blocked amount of money without undue delay, without prejudice to any other statutory or contractual rights, after the Bank has been notified of the exact amount to be paid or after the payment order has been received.

5 Rejection of card payments by the Bank

The Bank is entitled to reject a card payment if

- the cardholder has not proved his/her identity with the PIN or other authentication element,
- the payment is not within the card transaction limit applicable to the relevant card payment or the financial limit, or
- the card is blocked.

The cardholder will be notified accordingly via the terminal at which the card is being used or, in the case of online use, via the agreed method.

6 Execution period

The payment procedure is initiated by the creditor. Upon receipt of the payment order by the Bank, the Bank is obliged to ensure that the amount of the card payment is received by the creditor's payment service provider at the latest at the time stated in the List of Prices and Services (»Preis- und Leistungsverzeichnis«).

7 Financial limitations of use

The cardholder may only use the MasterCard within the card transaction limit and only in a manner that ensures that any expenditure accumulated via card transactions can be settled when it falls due.

The cardholder can reach an agreement with his/her Bank to alter his/ her card transaction limit.

Even if the cardholder does not remain within the financial limit, the Bank is entitled to be compensated for expenses resulting from the use of the MasterCard. The approval of individual MasterCard transactions leads neither to the granting of a credit nor to an increase in a previously agreed credit limit, but is done so in the expectation that any expenditure accumulated via the MasterCard can be settled when it falls due.

If the posting of MasterCard expenditure exceeds the cardholder's available account balance or a credit limit previously agreed for the account, the posting merely leads to a tolerated account overdraft.

8 Cardholder's duty of care and attention

8.1 Signature

The cardholder must sign the card on the signature strip immediately upon receipt.

8.2 Safe storage of the card

The card must be stored with particular care so as to prevent loss or misuse. In particular, it may not be left unattended in motor vehicles. Anyone who is in possession of the card will be able to misuse it.

8.3 Secrecy obligations regarding the PIN

The cardholder shall ensure that no third party has access to his/her PIN. In particular, the PIN may not be written on the card itself or be stored in any form whatsoever together with the card. Anyone who knows the PIN and gains possession of the card or knows the MasterCard number will be able to misuse the card (e.g. make cash withdrawals at cash dispensers).

8.4 Protection of authentication elements for online payment transactions

The cardholder shall take all reasonable precautions to protect his/her online payment authentication elements (see last subparagraph of No 3 of these Conditions) agreed with the Bank from unauthorised access. Otherwise, there is a risk that the authentication elements for online payment transactions may be misused or used in any other unauthorised way. In order to protect the individual authentication elements for online payment transactions, the cardholder must pay particular attention to the following:

(a) Elements of knowledge, such as the online password, must be kept secret; they must in particular

- not be communicated orally (e.g. by telephone or in person),
- not be passed on outside of online payment transactions in text form (e.g. by e-mail or messenger service),
- not be stored unsecured electronically (e.g. storage of the online password in plain text on the mobile device), and
- not be recorded on a device or kept as a transcript together with a device that serves as a possession element (e.g. mobile terminal) or to verify the inherence element (e.g. mobile terminal with application for credit card payment and fingerprint sensor).

(b) Possession elements, such as a mobile terminal, shall be protected from misuse, in particular it must be ensured

- that unauthorised persons cannot access the cardholder's mobile terminal (e.g. mobile phone),
- that other persons cannot use the credit card payment application (e.g. card app, authentication app) on the mobile device (e.g. mobile phone),
- that the application for online payment transactions (e.g. card app, authentication app) on the subscriber's mobile terminal is deactivated before the subscriber gives up possession of this mobile terminal (e.g. by selling or disposing of the mobile telephone), and
- that the evidence of the ownership element (e.g. TAN) passed on orally (e.g. by telephone) or in text form



(e.g. by e-mail, messenger service) outside the online payment processes.

(c) Elements of inherence, such as the cardholder's fingerprint, may only be used as an authentication element on a mobile terminal of the cardholder for online payment transactions if no other person's elements of inherence are stored on the mobile terminal. If the mobile device used for online payment transactions contains elements of inherence of other persons, the knowledge element issued by the Bank (e.g. online password) shall be used for online payment transactions and not the existence element stored on the mobile device.

8.5 Verification obligations for online payment transactions

If the cardholder is provided with information on the payment transaction (e.g. the name of the contracting company and the amount of the transaction) during online payment transactions, the cardholder must check this information for correctness.

8.6 Cardholder's obligation to report loss

(1) Should the cardholder become aware that his/her card is missing or has been stolen, or that the PIN, card or agreed elements of authentication for online payments have been misused or otherwise used without authorisation, the Bank, if possible the accountholding branch, or a representative office of the MasterCard organisation must be informed without delay to arrange for the MasterCard to be blocked. The cardholder will be informed separately of the contact data for a card-blocking notification. The cardholder must also report any theft or misuse to the police without delay.

(2) Should the cardholder suspect that a third party has come into possession of the card without authorisation or that the PIN, card or agreed elements of authentication for online payments have been misused or otherwise used without authorisation, he/she also has to issue a cardblocking notification without delay. For the replacement of a lost, stolen, misused or otherwise unauthorised card, the Bank shall charge the cardholder the fee stated in the Bank's »List of Prices and Services« (»Preis- und Leistungsverzeichnis«), which shall cover any costs directly and exclusively connected with the replacement. Sentence 1 shall not apply if the Bank is responsible for the circumstances which led to the issuance of the substitute card or if these circumstances are attributable to it.

(3) If a TAN generator or signature function for online banking is stored on the card, the blocking of the card will also entail a blocking of the online banking access.

(4) An additional company-generated application can only be blocked by the company that has stored the additional application on the chip of the MasterCard and to the extent that the company has provided for the relevant procedures to block its additional application. An additional Bank-

generated application can only be blocked by the card-

issuing Bank, subject to the agreement concluded with the card-issuing Bank.

(5) The cardholder has to notify the Bank without delay if he/she becomes aware of any unauthorised or incorrectly executed card transactions.

9 Payment obligation of the cardholder

The Bank has given contractual partners, and financial institutions accepting MasterCard at their cash dispensers, an undertaking to settle the transactions the cardholder carries out with the card. The Bank informs the cardholder at least once a month about all the expenses relating to the settlement of the card transactions via the communication channel agreed upon for account information. For cardholders that are not consumers, the communication channel and time intervals for information are agreed separately. The amount falls due after the Bank has issued a statement to the cardholder. Once the statement has been issued the card transactions are charged to the agreed settlement account.

Any objections or other complaints by the cardholder in respect of his/ her contractual relationship with a contractual partner where the card was used should be addressed directly to the contractual partner concerned.

10 Foreign currency conversion

When the card is used for transactions that are not denominated in euros, the account shall nevertheless be debited in euros. The conversion rate that is applied to transactions in foreign currencies shall be determined according to the List of Prices and Services (»Preis- und Leistungsverzeichnis«). Any change of the reference conversion rate as stated in the provision relating to the conversion will become effective immediately and without prior notification of the cardholder.

11 Charges

(1) The charges the cardholder owes to the Bank are determined on the basis of the Bank's List of Prices and Services (»Preis- und Leistungsverzeichnis«).

(2) Changes in charges for consumers: Changes in charges will be offered to the cardholder in text form no later than two months before their date of entry into force. If the cardholder has agreed an electronic communication channel (e.g. online banking) within the framework of the business relationship, the changes may also be offered through this channel.

The changes offered by the Bank shall only become effective if the cardholder accepts them. Any agreement on amending a charge that concerns a payment by the cardholder in excess of the charge for the principal service can only be expressly concluded with the consumer by the Bank.



The amendment of charges for the payment service framework agreement (giro contract) is governed by No. 12 (5) of the General Business Conditions (»Allgemeine Geschäftsbedingungen«).

(3) Changes in charges for customers who are not consumers: As regards charges and changes thereto for payments of cardholders that are not consumers, the provisions of No. 12 paragraphs 2-6 of the General Business Conditions continue to apply.

12 Cardholder's claims for a refund, correction and for damages

12.1 Refund in the event of unauthorised card transactions

In the event of an unauthorised card transaction in the form of

- a cash withdrawal, or
- the use of the card for payment at a contractual partner, the Bank has no right to claim a refund of its expenses from the cardholder. The Bank is obliged to refund the amount to the cardholder without delay and in full. If the amount was debited to an account, the Bank will ensure that the balance of the account is as it would have been without the unauthorised card transaction. This obligation must be fulfilled no later than the end of the business day as indicated in the Bank's List of Prices and Services (»Preis- und Leistungsverzeichnis«) which comes after the day on which the Bank was notified that the credit transfer is unauthorised, or the Bank has obtained knowledge thereof by some other means. If the Bank has informed a competent authority in writing of legitimate reasons for suspecting fraudulent conduct on the part of the customer, the Bank shall be required to consider and to fulfil its obligation arising from sentence 2 without delay if its suspicion of fraud is not confirmed.

12.2 Entitlement if an authorised card transaction is not executed, is executed incorrectly or is delayed

(1) In the event of the non-execution or incorrect execution of an authorised card transaction in the form of

- a cash withdrawal, or
- the use of the card for payment at a contractual partner, the cardholder can demand that the Bank refund the transaction amount without delay and in full insofar as the card transaction was not executed or was executed incorrectly. If the amount was debited to an account, the Bank will ensure that the balance of the account is as it would have been without the non-executed or incorrectly executed card transaction.

(2) Over and above paragraph 1, the cardholder can demand that the Bank refund charges and interest to the extent that these were charged to him/her or debited to his/her account in connection with the nonexecution or incorrect execution of the authorised card transaction.

(3) If the payment amount is received by the payee's payment service provider only after expiry of the execution period specified in Section I. 6 (delay), the payee may require his payment service provider to credit the payment amount to the payee's account as if the card payment had been properly executed. The obligation set out in sentence 1 does not apply if the cardholder is not a consumer.

(4) If an authorised card transaction was not executed or executed incorrectly, the Bank will retrace the card transaction at the cardholder's request and inform him/her of the findings.

12.3 Claims for damages by cardholders in the event of an unauthorised card transaction or the non-execution or incorrect execution of an authorised card transaction

In the event of an unauthorised card transaction or an authorised card transaction that is not executed, executed incorrectly or delayed, the cardholder can claim damages from the Bank for losses not already covered by Nos. 12.1 and 12.2. This does not apply if the Bank is not responsible for the violation of duties. In this context, the Bank is responsible for the fault of an intermediary as if it was the Bank's own fault unless the major reason for the fault lies with an intermediary selected by the cardholder. If the cardholder is not a consumer or the card is used outside Germany and in a country outside the European Economic Area (EEA)¹, the Bank's liability for the fault of an agency involved in the settlement of the payment transaction shall be limited to the careful selection and instruction of such agency. If the cardholder has contributed to the occurrence of any loss by any own fault, the principles of contributory negligence shall determine the extent to which the Bank and the cardholder shall have to bear the loss. Liability under this paragraph is limited to EUR 12,500 per card transaction. The limitation of liability to this amount does not apply

- to unauthorised card transactions,
- in the event of intent or gross negligence on the part of the Bank,
- to risks specifically taken on by the Bank, and
- to interest losses arising for the cardholder, insofar as the cardholder is a consumer.

12.4 Time limit for raising claims under Nos. 12.1 to 12.3

Claims against the Bank under Nos. 12.1 to 12.3 are excluded if, within a period of 13 months following the date on which the debit entry resulting from the card transaction has been made, the cardholder has not informed the Bank that the card transaction was not authorised, not executed or incorrectly executed. The 13-month period shall only begin if the Bank has notified the cardholder of the debit entry resulting

¹ The EEA currently comprises Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France (including French Guiana, Guadeloupe, Martinique, Mayotte, Réunion), Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovak Republic, Slovenia, Spain, Sweden and the United Kingdom of Great Britain and Northern Ireland.



from the card transaction via the relevant communication channel agreed upon for transaction information at the latest within one month of the debit entry; otherwise the period shall begin on the day of the notification. The cardholder may also raise claims under No. 11.3 after the end of the period as set out in sentence 1 if he/she was unable to meet the deadline through no fault of his/her own.

12.5 Right to claim a refund in the case of authorised card transactions for an unknown amount and time limit for raising the claim

(1) The cardholder can demand that the Bank refund the transaction amount without delay and in full if he/she has authorised a card transaction at a contractual partner such that

- the exact amount was not known when the transaction was authorised, and
- the payment transaction exceeds the amount that the cardholder would have expected, given his/her previous spending habits, the contents of the card agreement and the circumstances in the situation in question; reasons relating to any currency exchange are not taken into account if the reference exchange rate was used.

The cardholder is obliged to give the Bank an explanation of the circumstances upon which he/she is basing his/her claim for a refund.

(2) Claims for a refund expire if they are not raised with the Bank within eight weeks of the date on which the transaction is debited to the settlement account.

12.6 Exclusion of liability and objection

Claims of the cardholder against the Bank under Nos. 12.1 to 12.5 are excluded if the circumstances that give rise to a claim

- are the result of an unusual and unforeseeable event over which the Bank has no influence and the consequences of which the Bank could not have avoided with all due care and attention, or
- were brought about by the Bank due to statutory requirements.

13 Liability of the cardholder for unauthorised card transactions

13.1 Liability of the cardholder prior to the card-blocking notification

(1) If the cardholder loses his/her card or PIN, if the card or PIN are stolen or otherwise missing or if the card or agreed elements of authentication for online payments are otherwise misused and if this leads to unauthorised card transactions in the form of

- a cash withdrawal, or
- the use of the card for payment at a contractual partner, the cardholder is liable for any losses arising up to the time of the card-blocking notification up to an amount of EUR 150 irrespective of whether the cardholder is responsible for the card being lost, stolen or otherwise missing.

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

- it has not been possible for the cardholder to notice the loss, theft or any other misuse of the card or the agreed elements of authentication for online payments prior to the unauthorised use, or
- the loss of the card has been caused by an employee, an agent, a branch of the Bank or any other body to which the activities of the Bank have been outsourced.

(3) If the cardholder is not a consumer or the card is used outside Germany and in a country outside the European Economic Area, the cardholder shall be liable for losses arising as a result of unauthorised card transactions pursuant to paragraphs 1 over and above the maximum amount of EUR 50 if the cardholder has breached his/her obligations under these terms and conditions due to negligence. If the Bank has contributed to any losses by any own fault, the Bank shall be liable for any losses to the extent that it is responsible for them.

(4) In cases where unauthorised card transactions are made prior to the card-blocking notification and the cardholder has acted fraudulently, or intentionally or in gross negligence breached his/her duties of care and attention under these terms and conditions, the cardholder shall be fully liable in respect of any losses incurred as a consequence thereof. Gross negligence on the part of the cardholder can be deemed to have occurred, in particular, if

- he/she has culpably failed to notify the Bank or the representative office of the MasterCard organisation of the loss or, theft of the card or unauthorised use of the card without delay after becoming aware of it,
- the PIN or the agreed knowledge element for online payment transactions (e.g. online password) has been written on the card or stored together with the card (e.g. in the original letter that informed the cardholder of the PIN),
- the PIN or the agreed knowledge element for online payment transactions (e.g. online password) has been passed on to a third party, resulting in misuse of the card.

(5) Liability for losses incurred during the period to which the transaction limit relates shall be limited to the amount of the transaction limit specified for the card.

(6) The cardholder shall not be obliged to pay compensation for the damage in accordance with paragraphs 1,3 and 4 if the cardholder was unable to hand in the blocking notification because the Bank had not ensured the possibility of accepting the blocking notification.

(7) Notwithstanding paragraphs 1, 3 and 4, the cardholder shall not be liable to pay damages if the Bank has not requested the cardholder to provide strong customer authentication within the meaning of section 1 paragraph 24 of the German Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz – ZAG) or if the payee or his payment service provider has not accepted such strong customer



authentication even though 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 knowledge (something the cardholder knows, such as PIN or online password), possession (something the cardholder owns, such as credit card or mobile terminal) or inherence (something distinct to the cardholder, such as fingerprints).

(8) Paragraphs 2, 5 and 7 shall not apply where the cardholder has acted fraudulently.

13.2 Liability of the cardholder as from the card-blocking notification

As soon as the loss or theft of the card, the misuse or other unauthorised use of the card, PIN or agreed elements of authentication for online payments have been reported to the Bank or a representative office of the MasterCard organisation, the Bank shall assume any losses incurred afterwards as a result of transactions in the form of

- a cash withdrawal, or
 - the use of the card for payment at a contractual partner.
- If the cardholder acts with fraudulent intent, the cardholder shall also be liable for any losses incurred after the card-blocking notification.

14 Joint and several liability in the case of more than one applicant

Liabilities arising in connection with a MasterCard that was applied for by more than one applicant are of a joint and several nature, i.e. the Bank can request any applicant to satisfy all the claims. Each applicant can bring the contractual relationship to an end at any time by termination but only with effect for all the applicants.

Each applicant must ensure that the card issued to him/her is immediately returned to the Bank when termination becomes effective. Likewise, expenses arising from the further use of a card until it is returned to the Bank must be borne jointly and severally by the applicants. Irrespective of the foregoing, the Bank will take reasonable measures to prevent MasterCard transactions after the termination of the MasterCard contractual relationship.

15 Ownership and validity of the card

The card remains the property of the Bank. It is not transferable. The card is valid only for the period stated on it. The Bank is entitled to demand the return of an old card as soon as a new card has been issued to the cardholder or, at the latest, upon expiry of the old card. If the cardholder's entitlement to use the card ends prematurely (e.g. as a result of termination of the MasterCard agreement), the cardholder shall return the card to the Bank without delay. If any

additional company-generated applications are stored on the MasterCard, the cardholder must arrange for the company that stored the additional application on the MasterCard to immediately remove it. The possibility to continue using an additional Bank-generated application is governed by the contractual relationship between the cardholder and the card-issuing Bank.

The Bank reserves the right to exchange an old card for a new one at any time during a card's period of validity. This will not result in any costs for the cardholder.

16 Cardholder's right of termination

The cardholder can terminate the MasterCard agreement at any time without notice.

17 Bank's right of termination

The Bank can terminate the MasterCard agreement by giving reasonable notice of at least two months. The Bank will terminate the MasterCard agreement with a longer notice period if, following due consideration of the justified interests of the cardholder, this is deemed reasonable. The Bank can terminate the MasterCard agreement without notice if there is a reasonable cause which, even after due consideration of the justified interests of the customer, makes it unreasonable for the Bank to continue operating the MasterCard agreement.

A reasonable cause is deemed to exist in particular if the cardholder has provided incorrect information about his/her financial situation and the Bank has based its decision to conclude the MasterCard agreement on this information, or if the cardholder's financial situation deteriorates substantially or threatens to do so and thereby jeopardises the customer's ability to meet his/her obligations towards the Bank under the MasterCard agreement.

18 Consequences of termination

As soon as the MasterCard agreement is terminated, the MasterCard may no longer be used. The card shall be returned to the Bank immediately and without further request. If any additional company-generated applications are stored on the card, the cardholder must arrange for the company that stored the additional application on the MasterCard to immediately remove it. Depending on the provisions governing the relevant additional application, the cardholder may continue to use any additional Bank-generated applications.

19 Confiscation and blocking of the MasterCard

(1) The Bank is entitled to block the card and to initiate the confiscation of the card (e.g. by a cash dispenser),



- if it is entitled to terminate the Cardholder Agreement for reasonable cause,
 - if this is justified by factual reasons relating to the security of the card, or
 - if unauthorised or fraudulent use of the card is suspected.
- The Bank will notify the cardholder of the blocking if possible prior to but at the latest immediately subsequent to the blocking, stating the reasons for the blocking. The Bank will unblock the card or replace it with a new card, if the reasons for blocking the card no longer exist. In this case, too, the Bank will notify the cardholder without delay.

(2) If a TAN generator or signature function for online banking is stored on the card, the blocking of the card will also entail a blocking of the online banking access.

(3) If the cardholder has an additional application stored on a card, he/ she can no longer use the additional application after the card has been confiscated. If any additional company-generated applications are stored on the card when it is confiscated, the cardholder can ask the Bank to return such applications once the latter has received the card from the MasterCard contractual partner or financial institution that confiscated it. The Bank is entitled to comply with the cardholder's request to surrender additional company-generated applications by returning the card to the cardholder with all payment functions removed. The possibility to continue using an additional Bank-generated application stored on the card is subject to the rules governing the additional application in question.

II Additional applications

1 Storing additional applications on the card

- (1) The chip integrated in the credit card can also be used as a storage medium for an additional application generated by the Bank (e.g. a feature for the protection of minors) or by a company (e.g. an electronic ticket function).
- (2) The use of an additional Bank-generated application depends on the legal relationship between the cardholder and the card-issuing Bank.
- (3) The cardholder can use an additional company-generated application in accordance with the agreement concluded with the company. It is up to the cardholder to decide whether he/she wishes to use his/her card to store additional company-generated applications. An additional company generated application may be stored on the card at a company terminal as agreed upon by the cardholder and the company. Information exchanged at the company terminal is not disclosed to credit institutions.

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

With the chip integrated in the card, the card-issuing Bank only provides a technical platform enabling the cardholder to store additional company-generated applications on the MasterCard. Any services the company provides to the cardholder via the additional company-generated application are governed solely by the provisions of the agreement concluded between the cardholder and the company concerned.

3 Processing of complaints in respect of additional applications

(1) Any objections by the cardholder relating to the content of an additional company-generated application should only be addressed to the company that has stored the additional application on the card. The company shall process such objections on the basis of the data stored with it. The MasterCard may not be handed over to the company by the customer cardholder for the purpose of processing any complaints.

(2) Any objections by the cardholder relating to the content of an additional Bank-generated application should only be addressed to the Bank.

4 No entry of the PIN assigned to the cardholder by the Bank when using additional company generated applications

When storing, changing the contents of or using an additional company-generated application on the credit card, the PIN assigned to the cardholder by the card-issuing Bank is not to be entered. In case the company that has stored an additional company-generated application on the MasterCard allows the cardholder to secure access to such additional application using a means of identification of his choice, the cardholder may not use the PIN assigned to him/her by the card-issuing Bank to use the card's payment functions in order to secure the additional company-generated application.

5 Possibility to block additional applications

An additional company-generated application can only be blocked by the company that has stored the additional application on the chip of the MasterCard and to the extent that the company has provided for the relevant procedures to block its additional application. Additional Bank-generated applications can only be blocked by the Bank subject to the agreement concluded with the Bank.