Girocard (Debit Card)
Special Terms and Conditions

A. Guaranteed Types of Payment
B. Other Bank Services
C. Additional Applications
D. Amicable Dispute Resolution and Other Possibilities for Complaints

The present translation is furnished for the customer's convenience only. The original German text is binding in all respects.

In the event of any divergence between the English and the German texts, constructions, meanings, or interpretations, the German text, construction, meaning or interpretation shall govern exclusively.

A. Guaranteed Types of Payment

I. Scope of Application

Girocard is a debit card. Card Holder may use the Card for the below payment services if the Card and the terminals are equipped accordingly:

1 in connection with a personal identification number (PIN) with all German debit card systems:
a) for withdrawing cash at cash machines belonging to the German cash machine system showing the girocard logo;

b) for using it with retailers and services providers at automated tills belonging to the German girocard system showing the girocard logo ("Girocard Terminals");

c) for topping up prepaid mobile phone accounts at cash machines which a user has with a mobile phone operator if the cash machine operator offers such services and the mobile phone operator participates in the system.

2 in connection with a personal identification number (PIN) with third-party debit card systems:
a) for withdrawing cash at cash machines belonging to third-party cash machine systems if the card is equipped accordingly;

b) for using it with retailers and services providers at automated tills belonging to third-party systems if the card is equipped accordingly;

c) for topping up prepaid mobile phone accounts at third-party cash machines which a user has with a mobile phone operator if the cash machine operator offers such services and the mobile phone operator participates in the system, whereby Card acceptance by third-party systems is subject to the third-party system acceptance logo.

3 without using a personal identification number (PIN):
a) for contactless payment operations with retailers and services providers at automated tills belonging to the German girocard system showing the girocard logo for amounts of up to EUR 50 per transaction if the relevant automated tills do not require a PIN for contactless use;
b) for contactless payment operations with retailers and services providers at automated tills belonging to third-party debit card systems for amounts of up to EUR 50 per transaction if the relevant automated tills do not require a PIN for contactless use, whereby Card acceptance by third-party systems is subject to the third-party system acceptance logo;

c) outside these payment services and without a Bank guarantee being connected to the function, as a storage device for additional applications

- offered by Bank subject to the agreement concluded with Bank ("Bank-Generated Additional Applications") or
- offered by several retailers and services providers subject to the agreement which they concluded with Card Holder ("Company-Generated Additional Applications").

II. General Rules

1 Card Issuance
The girocard may be issued as a physical or digital card to be stored on a telecommunications, digital or IT device ("Mobile Terminal"). These Special Terms and Conditions shall apply to both types of card, unless expressly regulated otherwise; usage instructions concerning the digital card must be additionally considered.

2 Card Holder and Authority
The Card may be used for the account indicated thereon and, if applicable, for additional accounts agreed upon to which Card Holder has access. It may only be issued in the name of Card Holder or other individuals whom Card Holder granted an account authorisation. Should Card Holder revoke such account authorisation, he/she shall be responsible for having the authorised individual to whom a Card was issued return the Card to Bank. After such account authorisation revocation, Bank shall electronically block the Card for usage at cash machines and automated tills. Company-Generated Additional Applications can only be blocked by the company which stored such additional application on the Card chip, which shall only be possible if such company is able to actually block such additional services. Bank-Generated Additional Services, in return, may only be blocked by Bank and shall be subject to the contract between Bank and Card Holder. So long as the Card has not yet been returned, it is possible to continue to use any additional applications stored on the Card.

3 Financial Limits

Card Holder's Card-based transactions shall be limited to the relevant account balance or any other facilities which were previously granted to the relevant account. Even if Card Holder does not comply with this limit, Bank shall be entitled to request compensation for expenses resulting from Card usage. Bookings of such transactions on the account lead to tolerated overdrafts.

4 Translation of Foreign Currency Amounts

If Card Holder uses the Card for transactions not denominated in Euro, the account shall still be charged with the amount in Euro. Exchange rates for foreign currency transactions are indicated in the "Prices and Services Schedule". Changes to reference exchange rates indicated in these translation regulations shall come into effect immediately and without previous notification of Customer.

5 Girocard Return

The Card shall remain Bank's property, it may not be transferred and it is valid only during the period indicated thereon.

Upon issuance of a new Card, in no case later than upon termination of the old Card, Bank may request the old Card to be returned and/or the digital Card to be deleted, but they may also provide for this themselves. Should the Card usage right terminate prematurely (e.g. due to closing of the account or card contract cancellation), Card Holder must immediately return the Card to Bank and/or delete the digital card. Card Holder must request the company which stored any Company-Generated Additional Applications on the Card to immediately remove such applications. The possibility of continued Bank-Generated Additional Applications usage shall depend on the contract between Card Holder and Bank.

6 Girocard Blocking and Withdrawal

(1) Bank may block the Card and have it withdrawn (e. g. through cash machines) and/or request or provide themselves for the deletion of the digital card:

- if they are entitled to Card contract cancellation for cause;
- if factual reasons relating to Card security justify this; or

- if there is reason to believe that unauthorised or fraudulent Card usage occurred.

Bank shall inform Card Holder about this by indicating the relevant reasons prior to – if possible – and not later than immediately after blocking or deleting the Card. Bank shall deblock or replace the Card by a new one if the reasons for Card blocking no longer exist and inform Card Holder about his as quickly as possible.

(2) Should the Card include an online banking TAN generator or signature function, blocking the Card leads to these online banking functions being blocked, too.

(3) If Card Holder had any additional applications installed on his/her Card, card withdrawal has the effect of him/her no longer being able to use these additional application. Card Holder may request the card-issuing institution to return any Company-Generated Additional Applications installed on the Card after the institution has received the Card from the office which withdrew the Card. Bank shall be entitled to fulfil the request for the return of Company-Generated Additional Applications by providing Card Holder with a Card which no longer includes the payment functions. The possibility of continued Bank-Generated Additional Applications usage shall depend on the rules regulating these additional applications.

7 Card Holder's Duty of Care and Cooperation

7.1 Signature

Should the Card have a signature field, Card Holder must immediately sign the Card on that signature field.

7.2 Secure Girocard Storage

Particular care must be applied to card storage to prevent that it is lost or misused. In particular, it may not be left unattended in a car since it (e. g. in the girocard system) can be misused. Also, every individual disposing of the Card may execute transactions at automated tills without the need for a PIN until the Card is blocked or deleted.

7.3 Personal Identification Number (PIN) Secrecy

Card Holder must ensure that no other individual gets to know his/her personal identification number (PIN). In particular, the PIN may not be noted on the Card itself or, regarding digital Cards, stored on the same Mobile Terminal which is used for the digital card or in any other way together with it. The reason is that any individual knowing the PIN and having access to the Card is able to make transactions (such as withdrawing cash) at the expense of the account indicated on the Card and, if applicable, to any additional account to which Card Holder has access. If Card Holder uses a digital card and if Card Holder is able to secure access to the Mobile Terminate or any other communication device by selecting credentials, Card Holder may not use the PIN required for card usage also for protecting access.

7.4 Duty to Provide Information and Notifications

(1) Once Card Holder becomes aware of having lost his/her Card and/or Mobile Terminal or them being stolen and/or his/her Card or Mobile Terminal being misused or used in any other unauthorised manner, they shall immediately inform Bank, that is, if possible, the account-holding branch ("Blocking Notification"). Card Holder may make such Blocking Notification, at any time, also towards the Central Card Assistance Service [*Zentraler Sperrannahmedienst*] (by telephone at 116 116 from German territory and at +49 116 116 from abroad [a different country code may apply]). In this case, blocking the Card is possible only if Bank was provided with the name – including the bank code – and the account number. The Central Card Assistance Service will cancel any Cards relating to the affected account and, if applicable, access to additionally defined accounts to which Card Holder has access through his/her Card so that it can no longer be used for cash machines and automated tills. For limiting cancellation to the lost Card, Card Holder must contact their Bank, that is, the account-holding branch, if possible. Card Holder must immediately report any card loss or theft with the police.

(2) If there is reason for Card Holder to be believe that any other individual illegally gained access to his/her Card or that his/her Card or PIN was misused or used in an unauthorised manner, he/she must also immediately make a Blocking Notification.

(3) When replacing a Card which had been lost, stolen, misused or used in any other unauthorised manner, Bank may charge the fee to Card Holder which is indicated in the Bank's "Prices and Services Schedule" in terms of sec. 675 l para. 1 *BGB* [*Bürgerliches Gesetzbuch* – German Commercial Code] if the reasons leading to card replacement are within Card Holder's control and if Bank is not obligated to issue such replacement card.

(4) Should the Card include an online banking TAN generator or signature function, blocking the Card leads to these online banking functions being blocked, too.

(5) By requesting Bank or the Central Card Assistance Service to cancel the Card, access to the Mobile Terminal on which a digital card is installed will not be blocked. However, only the relevant function provider is able to block any other functions installed on the Mobile Terminal on which the digital card is stored.

(6) Company-Generated Additional Applications can only be blocked by the company which stored such additional application on the Card chip, which shall only be possible if such company is able to actually block such additional services. Bank-Generated Additional Services, in return, may only be blocked by Bank and shall be subject to the contract between Bank and Card Holder.

(7) Account Holder shall immediately notify Bank of any unauthorised or incorrectly executed card transactions immediately after he/she became aware of this.

8 Card Payments Authorisation by Card Holder

When using the Card by inserting it into automated tills or when making contactless payments by holding it close to the automated till, Card Holder grants his/her approval ("Authorisation") to executing a card payment. If a PIN is required for this, approval is granted only after the PIN was entered. Once Card Holder granted his/her approval, a card payment can no longer be revoked. This authorisation also includes an express approval of Bank having the right to call off, process, transmit and store any of Card Holder's personal data required for card payment execution.

9 Blocking Available Balances

Bank shall be entitled to block any balances available on Card Holder's account within the framework of financial limits (A. II. 3) if:
- the payment transaction was initiated by the payment recipient; and
- the exact amount of balances to be blocked was approved by Card Holder.

Save any other statutory or contractual rights, Bank shall release any blocked balances immediately after they were informed about the exact payment amount.

10 Rejection of Card Payments by Bank

Bank shall have a right to reject card payments if:

- the Card Holder failed to authorise the card payment in terms of A. II 8;
- the cash limit for card payments or the financial limit was not complied with; or

- the Card was blocked.

Card Holder shall be informed about this via the terminal at which the Card is used.

11 Execution Period

The payment transaction is initiated by the payment recipient. Once Bank received the relevant payment order, they must ensure that the payment recipient's payment services provider receives the card payment not later than at the time indicated in the "Prices and Services Schedule".

12 Fees and Fee Changes

(1) The fees which Card Holder must pay to Bank are listed in the "Prices and Services Schedule".

(2) Account Holder shall be informed in writing about changes to the fees not later than two months prior to the new fees coming into effect. Should Account Holder and Bank agree upon electronic communication for the business relationship (such as online banking), such notification may also be provided by electronic means. Account Holder may either accept or reject any such changes prior to them becoming effective. Account Holder shall be considered to have agreed if they failed to reject prior to the proposed date of such changes coming into effect; in their offer, Bank shall separately inform them about this.

(3) If Account Holder is offered any fee changes, they may cancel this business relationship prior to the changes becoming effective, with no notice period and no fees; in their offer, Bank shall separately inform them about special right to cancellation.

(4) The provisions under no. 12 para. 2 through 6 of the General Terms and Conditions shall continue to apply to fees and fee changes for payments from account holders who are no consumers.

13 Card Payment Process Information Provided to Account Holder

Bank shall inform Account Holder at least once a month about the execution of card payments in the manner which they had agreed upon for account information provision. It shall be possible to separately agree upon the manner and intervals of information provision with account holders who are no consumers.

14 Account Holder's Reimbursement, Correction and Compensation Claims

14.1 Compensation for Unauthorised Card Transactions

In the event of unauthorised Card transactions, such as in the form of

- cash withdrawals at cash machines
- usage of the Card at automated tills from retailers and service providers

- usage of the Card for topping up prepaid mobile phone accounts

Bank has no claims against Account Holder for compensation of their expenses. Bank shall be obligated to refund such amount to Account Holder without any deductions. If the amount was charged to Card Holder's account, Bank shall restore the account status which it would have had if the unauthorised card transaction had not been executed. This duty must be fulfilled, at the latest, by the end of the business day in terms of the "Prices and Services Schedule" following the day on which Bank was informed that the card transaction had not been authorised or on which Bank became aware of this in any other manner. If Bank communicated to the authority in charge in writing justified reasons according to which Card Holder engaged in fraud, Bank must immediately review and fulfil their duty under sent. 2 if the suspected fraud is not confirmed.

14.2 Claims Regarding Failed, Incorrect or Delayed Execution of Authorised Card Transactions

(1) If authorised card transactions, such as in the form of
- cash withdrawals at cash machines
- usage of the Card at automated tills from retailers and service providers
- usage of the Card for topping up prepaid mobile phone accounts

were executed not at all or not correctly, Account Holder may request Bank to immediately refund the transaction amount without any deductions to the extent that such card transaction failed or was incorrect. If the amount was charged to Card Holder's account, Bank shall restore the account status which it would have had if the failed or incorrect card transaction had not occurred.

(2) In addition to para. 1, Account Holder may request Bank to refund the fees and interest which they were charged with or which were deducted from their account in relation to the failed or incorrect execution of authorised card payments.

(3) Should the payment recipient's payment services provider receive the transaction amount only after the execution period in terms of A. II. 11 (Delay) terminated, the payment recipient may request their payment services provider to credit the transaction amount to the payment recipient's account as if the card payment had been correctly executed.

(4) If an authorised card payment was executed not at all or not correctly, Bank shall, upon Card Holder's request, review such card transaction and inform Card Holder about the relevant results.

14.3 Account Holder's Compensation Claims due to Violation of Duties

In the event of unauthorised card transactions and/or failed, incorrect or delayed execution of authorised card transactions, Account Holder may request compensation from Bank for any damage which is not included under A. II. 14.1 or 14.2; this shall not apply for duty violations beyond Bank's control. In this case, violations of any intermediaries involved shall be deemed Bank's own violations, unless the substantial reason can be attributed to such intermediary which Card Holder indicated. Should the account holder be no consumer or should the Card be used outside Germany and the European Economic Area, Bank's liability for culpability with regard to parties involved in the transaction process shall be limited to diligent selection and instruction of such party. Should Card Holder have culpably contributed to causing any damage, the extent of Bank's and Account Holder's liability shall depend on the contributory negligence principles. Liability in terms of this paragraph shall be limited to EUR 12,500 for each Card transaction. This amount-based liability limitation shall not apply to:

- unauthorised card transactions;
- intentional or grossly negligent behaviour of Bank;
- risks which Bank particularly accepted; and
- interest damage incurred by Account Holder if they are a consumer.

14.4 Liability Exclusion and Preclusion from Objection

(1) Claims in terms of A. II. 14.1 through 14.3 shall be excluded if Account Holder fails to inform Bank about any unauthorised, failed or incorrect card transaction 13 months from the day of charging the relevant Card transaction at the latest. This 13-month period shall only commence if Bank notified Account Holder of the debit entry resulting from the card transaction via the agreed account information communication channel not later than one month from the debit entry; otherwise, this period shall commence upon information provision. Account Holder may assert liability claims in terms of A. II. 14.3 also once the period under sent. 1 is over if they, with no fault of their own, were prevented from compliance.

(2) Account Holder's claims against Bank shall be excluded if circumstances establishing such claim

- are based on unreasonable and unforeseeable events beyond Bank's control and if it would have been impossible to prevent the consequences despite applying a reasonable level of diligence; or
- were established by Bank due to a statutory obligation.

15 Account Holder's Liability for Unauthorised Card Transactions

15.1 Account Holder's Liability Until Blocking Notifications

(1) If Card Holder loses his/her Card or PIN, if they are stolen from him/her, go astray for any other reason or are misused and if this results in unauthorised Card transactions, such as in the form of

- cash withdrawals at cash machines
- usage of the Card at automated tills from retailers and service providers
- usage of the Card for topping up prepaid mobile phone accounts

Account Holder shall be liable for any damage which are caused until their Blocking Notification submission to the maximum amount of EUR 50. Liability in terms of para. 6 for intention, gross negligence and fraud shall not be affected by this.

(2) Liability for Account Holder in terms of para. 1 shall be excluded if:

- it was impossible for Card Holder to become aware of having lost the Card, it being stolen or gone astray in any other manner or it being misused prior to the relevant unauthorised card transaction; or
- such card loss was caused by a Bank employee, agent or branch or by any other offices which were commissioned with Bank's activities. Liability in terms of para. 6 for intention, gross negligence and fraud shall not be affected by this.

(3) Should Account Holder be no consumer or should the Card be used outside Germany and the European Economic Area, Account Holder shall be liable for any amounts exceeding the maximum amount of EUR 50 for any damage resulting from unauthorised card transactions in terms of para. 1 and 2 if Card Holder negligently failed to fulfil their duties under these terms and conditions. If Bank contributed to causing any damage by violating their duties, they shall be liable for the relevant damage to the extent of their contributory negligence.

(4) Bank refrains from requesting Customer to bear a maximum share of EUR 50 of the damage in terms of para. (1) above and shall bear the entire damage resulting from unauthorised card transactions until Blocking Notification receipt if Card Holder did not negligently violate his/her duty of care and cooperation pursuant to A. II. 7.

(5) Account Holder shall not be obligated to compensate the damage in terms of para. 1 and 3 if Card Holder was unable to submit a Blocking Notification due to Bank not ensuring acceptance of such notification which lead to the damage.

(6) If unauthorised transactions occur prior to Blocking Notification, if Card Holder intentionally or grossly negligently violated his/her contractual duty of care or acted in a fraudulent manner, Account Holder shall bear the full extent of the damage. Cases of gross negligence for Card Holder shall particularly exist if he/she:

- culpably failed to notify Bank or the Central Card Assistance Service of loss, theft or improper transactions immediately after he/she became aware of this;
- recorded his/her personal identification number on the physical card or stored this together with the physical card (such as in the original letter communicated to Card Holder);
- stored his/her personal identification number for the digital card on his/her Mobile Terminal; or
- communicated his/her personal identification number to any other individual who misused this and caused the damage.

Liability for damage caused during the cash limit period shall be limited to the cash limit applicable to the relevant Card.

(7) If Bank failed to request strong customer authentication in terms of sec. 1 para. 24 of the German Financial Services Supervision Act [*Zahlungsdiensteaufsichtsgesetz*] or if this is rejected by the payment recipient of their payment services provider despite Bank being legally obligated to strong customer authentication, Card Holder's and Bank's liability shall, in deviation from para. 1 through 6, depend on the provisions under sec. 675 v para. 4 *BGB*.

15.2 Account Holder's Liability from Blocking Notifications

Once Bank or the Central Card Assistance Service is notified of the Card or the PIN being lost, stolen, misused or used in any other unauthorised manner, Bank shall be liable for any subsequent transactions, such as in the form of

- cash withdrawals at cash machines
- usage of the Card at automated tills from retailers and service providers
- usage of the Card for topping up prepaid mobile phone accounts

which cause any damage. Should Card Holder act fraudulently, he/she shall continue to be liable for any damage after he/she submitted a Blocking Notification.

III. Special Rules for Individual Types of Use

1 **Cash Machine Services and Usage at Automated Tills from Retailers and Service Providers**

1.1 Girocard Cash Limit

Card Holder shall be entitled to transactions at cash machines and automated tills only within the framework of the cash limit applicable to the Card. Whenever he/she uses the Card at cash machines and automated tills, Bank checks whether or not the card cash limit has already been fully utilised through previous transactions. Transactions due to which the card cash limit would be exceeded will be rejected irrespective of the current account balance and any loans granted for the relevant account. Card Holder may use the card cash limit only within the framework of their account balance or a facility which was previously granted for the relevant account. The card-holding branch and Account Holder may agree upon changing the card cash limit for any and all Cards which were issued for his/her account. Any representative who was provided with the Card may only agree upon a reduction in this regard.

1.2 Wrong Identification Number Entries

After Card Holder entered a wrong identification number three times in a row, the Card can no longer be used for cash machines and automated tills for which PIN entry is required in relation to card usage. In this case, he/she must contact Bank, that is, the account-holding branch, as early as possible.

1.3 Bank's Payment Duties; Objections

Bank undertook towards cash machine and automated tills operators to pay the relevant transactions amounts to them which Card Holder generated by using his/her Card. Card Holder's objections and any other complaints based on the contractual relationship with the company operating an automated till providing for cashless payments must be directly asserted to such company.

1.4 Automated Tills Pre-Selection

Retailers and services providers may, with regard to card types accepted by them, install mechanisms in their automated tills providing for a pre-selection of certain payment brands or applications. In this regard, they may not prevent Card Holder from overriding this pre-selection.

2 Topping Up Prepaid Mobile Phone Accounts

2.1 Service Description

By using his/her Card and personal identification number (PIN) Card Holder may use cash machines for topping up prepaid mobile phone accounts with mobile phone operators on which prepaid phone value units are stored, within the cash limit granted by his/her bank (A. III. 1.1) and at the expense of the account indicated on the Card. However, this shall be subject to the cash machine selected by Card Holder providing for such top-up function and mobile phone operator managing the prepaid mobile phone account to be topped up participating in the system. For topping up his/her prepaid mobile phone account, Card Holder must select the "Topping Up Prepaid Mobile Phone Account" menu item which is displayed, enter his/her mobile phone number and select displayed top-up amount on display. After top-up authorisation by Card Holder's Bank, the prepaid mobile phone account with the mobile phone operator will be topped up. Based on this procedure, Card Holder may top up his/her own prepaid mobile phone account and those of third parties. Should Bank reject top-up authorisation due to, including, without limitation, insufficient funds, a rejection notice will be displayed.

2.2 Wrong Identification Number Entries

After Card Holder entered a wrong identification number three times in a row, the Card can no longer be used for cash machines. In this case, he/she must contact Bank, that is, the account-holding branch, as early as possible.

2.3 Bank's Payment Duties; Objections

Bank is contractually obligated to pay any prepaid mobile phone account top-up amounts which were authorised by Card Holder; such payment duty shall be limited to the authorised amount. Card Holder's objections and any other complaints based on the contractual relationship with the mobile phone operator manging the prepaid account must be directly asserted to the relevant mobile phone operator.

B. Other Bank Services

If equipped accordingly, Card Holder may use the Card for the below services:

1 Entry of Transfer Orders at Self-Service Terminals

1.1 Service Description

Based on his/her Card and personal identification number, Card Holder may use Bank's self-service terminals to enter transfer orders within a cash limit of EUR 1,000 per day, unless Account Holder and Bank agreed upon other cash limits.

1.2 Transfer Execution

Transfer execution shall be subject to the Special Transfer Transactions Terms and Conditions separately agreed upon.

1.3 Duty of Care and Cooperation

The duty of care and cooperation under A. II. 7.2 through 7.4 shall additionally apply to Card usage.

1.4 Wrong Identification Number Entries

The regulations under A. III. 1.2 shall apply.

1.5 Account Holder's Liability for Unauthorised Transactions

Account Holder's liability for unauthorised transactions through self-service terminals shall be subject to the rules under A. II. 15; however, in deviation from A. II. 15.1 para. 6, Account Holder's liability shall be limited to EUR 1,000 per calendar day and, if any other cash limit was agreed in terms of B. 1.1, this relevant cash limit.

2 Self-Service Savings Transactions

2.1 Service Description

Owners of a savings account may, through their Cards and personal identification numbers, use cash machines for transactions on savings accounts which were released for these purposes based on a special agreement with Bank ("Self-Service Savings Transactions"); the savings account holder shall be exclusively granted releases for Self-Service Savings Transactions. The extent to which representatives may use Self-Service Savings Transactions shall depend on the respective agreements between Bank and Account Holder.

In the context of Self-Service Savings Transactions, it is possible to withdraw money from savings accounts at a cash machine. Concerning savings account transactions at cash machines, Bank and Account Holder shall agree upon a cash limit applicable to a certain period. Withdrawals due to which this cash limit would be exceeded will be rejected and it shall be limited to the contractual service regarding Self-Service Savings Transactions withdrawals.

2.2 Duty of Care and Cooperation

The duty of care and cooperation under A. II. 7.2 through 7.4 shall additionally apply to Card usage.

2.3 Wrong Identification Number Entries

The regulations under A. III. 1.2 shall apply.

2.4 **Account Holder's Reimbursement and Compensation Claims**

The regulations under A. II. 14 shall apply.

2.5 Account Holder's Liability for Unauthorised Transactions

Account Holder's liability for unauthorised transactions shall be subject to the rules under A. II. 15; however, in deviation from A. II. 15.1 para. 6, Account Holder's liability shall be limited to the cash limit applicable to Self-Service Savings Transactions (B. 2.1).

2.6 "SparCard Special Terms and Conditions" Applicability

The "SparCard Special Terms and Conditions" shall additionally apply to the extent identified for Self-Service Savings Transactions.

C. Additional Applications

1 Storage of Additional Applications on the Girocard

(1) Card Holder may use the Card chip as a storage device for Bank-Generated Additional Applications (such as for youth protection purposes) or Company-Generated Additional Applications (such as in the form of an electronic ticket).

(2) Bank-Generated Additional Applications usage shall depend on the legal relationship between Card Holder and Bank. Card Holder may use Company-Generated Additional Applications subject to a contract concluded with the relevant company. Card Holder shall decide whether or not he/she wants to store any Company-Generated Additional Applications on his/her Card. Such services shall be stored on the Card at the company's terminal after consultation between Card Holder and the company. Financial institutions have no information about the contents of data communicated at the company terminal.

2 Company Responsibility for the Contents of Company-Generated Additional Applications

Based on the Card chip, the card-issuing bank only provides a technical platform enabling Card Holder to store Company-Generated Additional Applications. Services which a company provides to Card Holder through any Company-Generated Additional Services shall be exclusively subject to the contents of the contractual relationship between Card Holder and the company.

3 Additional Applications-Related Objections Processing

(1) Card Holder may raise objections relating to Company-Generated Additional Application contents only towards the company which stored the additional applications on the Card. The company shall process such objections based on any data stored by them. Card Holder may not hand the Card over to the company for complaint processing purposes.

(2) Card Holder may raise objections relating to Bank-Generated Additional Application contents only towards Bank.

4 No Entry of Customer's PIN Provided by Bank for Company-Generated Additional Applications

For storing, changing their contents or using any Company-Generated Additional Applications on the Card, there is no need to enter the PIN which the card-issuing bank assigned to Card Holder. If the company storing a Company-Generated Additional Application on the Card enables Card Holder to protect access to such additional applications through separate credentials, Card Holder may not use the PIN to protect the Company-Generated Additional Applications which the card-issuing bank assigned to him/her for payment applications.

5 Additional Applications Blocking Possibility

Company-Generated Additional Applications can only be blocked by the company which stored such additional application on the Card chip, which shall only be possible if such company is able to actually block such additional services. Bank-Generated Additional Services, in return, may only be blocked by Bank and shall be subject to the contract between Bank and Card Holder.

D. Amicable Dispute Resolution and Other Possibilities for Complaints

For resolving any disputes with Bank, Customer may apply to the dispute resolution or complaints office indicated in the "Prices and Services Schedule" in more detail.