

## Conditions of Use for Services for Electronic Functionalities

### 1. Available services

Cornercard (hereinafter referred to as the "Bank") makes available to holders of business credit and prepaid cards, as well as personal credit and prepaid cards (hereinafter referred to as the "Cardholder") certain services for electronic functionalities, which may vary depending on the type of card and type of Cardholder. These services are available for all end devices supported by the Bank that can access electronic networks (Internet, SMS, etc.) via cell-phone networks or using other forms of electronic access. With the aid of these services, the Cardholder can view, in particular, his or her card usage and respective debits as well as any related messages. Furthermore, the Cardholder can use these services to take advantage of the security standards developed by Visa and Mastercard (Verified by Visa and Mastercard Identity Check) when making transactions on the Internet. Using these services, the Cardholder can call up and view all of the information and transactions that were processed by the Bank as of the previous working day. In the event of any inconsistencies between the information called up electronically and the Bank's internal accounting data, the latter data will always be decisive. The Bank reserves the right to, at its discretion, expand, reduce, modify, and/or interrupt its offer of services for electronic functionalities at any time. The Bank accepts no liability for any damage arising out of the related blocking or interruption of these services.

### 2. Electronic communications

The Bank is entitled to use the electronic contact data disclosed by the Cardholder or the Company (cell-phone number, e-mail address, etc.) for the purpose of sending messages and offers of a general nature as well as specific information related to the card and the transactions executed. The Cardholder and the Company shall not, under any circumstances, send personal data, card-specific or other confidential information via conventional e-mail. Unless expressly stated otherwise, the Bank does not accept any orders or instructions that it receives by e-mail or via any other electronic transmission system. Accordingly, no liability arises for the Bank in connection with **messages sent to it via any electronic means by the Cardholder or any third party.**

### 3. Security and identification procedures

Access to the services for electronic functionalities is regulated by a combination of various security procedures (authentication via SMS, generation of codes using specific authentication devices, passwords, etc.), which the Bank has defined and regarding which it has informed the Cardholder in a suitable manner. Identification may occur on individual security levels or a combination thereof. The Bank reserves the right to modify the procedures and identification measures used to regulate the access to and use of the individual services for electronic functionalities.

### 4. Authentication

Anyone who has been authenticated by using security procedures that are valid at the time of use may access and use the services for electronic functionalities of the Bank, as provided under section 3 of these Conditions (**self-authentication**). The Bank is therefore expressly released from any other obligation to verify, independently of any internal relationship between the Bank and Cardholders, and regardless of any deviating provisions set forth in forms issued by the Bank (card applications, etc.). The Bank reserves the right, however, to deny access to the services for electronic functionalities at any time and without providing reasons. **All transactions executed and charges debited against the card after this authentication/identification are attributed to the Company or the respective Cardholder, or the holder of the principal card as well in the case of a partner card, which is issued without its own spending limit and its own monthly statements; the Cardholder or, as the case may be, the holder of the principal card unconditionally accepts these as legally valid and binding. The Bank accepts no responsibility for any abuse by third parties.**

### 5. Security; obligations of due diligence

The Cardholder and the Company are aware that, due to the open configuration of electronic networks, it is possible for third parties to gain unauthorized access to the connection between his or her end device and the Bank's informatic system. Consequently, the Cardholder shall carefully store anything related to the security of his or her identification or end devices and anything used for authentication purposes in accordance with section 3. Therefore, the Cardholder undertakes to, in particular:

- ensure that any security procedures supplied by the Bank pursuant to section 3 **are not noted anywhere and that they are not disclosed or made accessible to third parties, even if such parties should identify themselves as employees of the Bank;**
- notify the Bank without delay if the electronic addresses registered with the Bank (cell-phone number, e-mail address, etc.) are changed;
- notify the Bank immediately in the event of loss or theft of the credit or prepaid card, the electronic end device (in particular the cell phone or other mobile end device), or the SIM card, etc.; the same obligation applies where abuse of these is suspected;
- regularly check the end device, which is used to access the services for electronic functionalities, for viruses, Trojan horses, and other malicious software. Furthermore, the Bank recommends using the latest version of the applications and operating system that is available for your end device and, if possible, activating the password lock on the end device (for example screen-saver password).

Should the Cardholder change the device settings of his or her end device in order to gain unlimited access to its functionalities (for example, jailbreaking for iOS devices or rooting for Android devices) he or she thus relinquishes the security features installed by the manufacturer. The Cardholder is liable to the Bank for any consequences arising out of any such changes to device settings. Therefore, the Bank strongly advises against any such steps and reserves the right in this case to block access to the services for electronic functionalities.

Links from the Bank's website or applications to third-party websites are used at the Cardholder's own risk. The Bank accepts no liability whatsoever for the content of any such websites or for any products or services these may offer.

**The Bank assumes no liability for any consequences arising from noncompliance with these obligations of due diligence, from the loss or abuse of the end devices, the Cardholder's electronic addresses, or the authentication devices supplied to the Cardholder by the Bank.**

### 6. Liability

Subject to the condition that the Cardholder has fulfilled his or her obligations of due diligence pursuant to section 5 and no other legal claims can be made against him or her (irrespective of the grounds therefor), the Bank is liable for direct damage arising immediately as a consequence of the use of the services for electronic functionalities provided that such damage is caused by errors or defects attributable exclusively to the Bank or is otherwise within its sphere of risk. Damage which is a consequence of mistakes, service interruptions, malfunctions, errors, defects, or interception by third parties during the transmission or processing of data via public telecommunication systems or networks does not fall within the Bank's sphere of risk. The Bank is not liable for indirect damage of any kind. Similarly, the Bank is not liable for direct damage covered by insurance. The Cardholder shall report any damage to the Bank without delay.

### 7. Fees

The applicable fees for the use of the Bank's services for electronic functionalities in Switzerland and abroad may be viewed at [cornercard.ch/e/gtc](http://cornercard.ch/e/gtc).

### 8. Amendment of the Conditions of Use

The Bank reserves the right to amend these Conditions of Use at any time. The Cardholder and the Company will be notified of such amendments by circular letter or in some other appropriate form. The amendments are deemed to have been accepted unless the Cardholder raises an objection in writing within 30 days of notification. In the event that the Cardholder objects to an amendment, the Bank reserves the right to block his or her access to its services for electronic functionalities or to terminate this access.

### 9. Activation, duration and other conditions

The Cardholder may apply to use the Bank's services for electronic functionalities at any time. This access may also be activated or deactivated (also by the Bank) at any time. Unless otherwise provided in these Conditions, the Cardholder's access to the Bank's services for electronic functionalities remain active until the expiration of the relevant card. The cardholder is aware that, in the event of cancellation or dissolution of the card contract, he will no longer have access to the electronic functionalities. These Conditions replace all prior Conditions of Use governing the same matters. The **General Terms and Conditions for the Visa and Mastercard credit and prepaid cards of Cornercard** apply in full to any matter not covered by these Conditions of Use.  
Version PB/03-B00T-1\_CH

Cornèr Banque SA – Cornèrcard – Via Canova 16 – 6901 Lugano