Conditions of Use for Services for Electronic Functionalities

1. Internet-accessible functionalities
Electronic functionalities are offered by Cornèr Bank Ltd. (hereinafter "the Bank") in connection with Diners Club credit cards from Cornèr Bank Ltd. (hereinafter "card(s)") for the respective private and corporate cardholders (hereinafter "Cardholder(s)") through contractual partners. These services are accessible via the Internet, and, in particular, they allow Cardholders (and, for corporate clients, also the company) to view card usage and respective debits. This information pertains to transactions recorded by the Bank or its partners up to the preceding business day. In the event of discrepancies with the Bank's internal accounting, the latter shall prevail. Cardholders and/or the company shall be fully responsible for any liabilities and/or consequences arising from the use of electronic functionalities. The Bank reserves the right to expand, reduce, modify, and/or suspend the range of functionalities without providing reasons. The Bank declines any responsibility for any damages arising from such a block or suspension. Functionalities may vary depending upon the type of card and/or the type of Cardholder.

2. Electronic communications
The Bank is entitled to use the electronic contact data disclosed by the Cardholder (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 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
Access to electronic functionalities occurs on the basis of security features adopted by the Bank, in particular the combined use of two or more of the following in conjunction with instructions properly provided by the Bank:

- a user -ID
- a personal password freely chosen by the Cardholder
- one of the following additional dynamic authentication methods recommended by the Bank, specifically:
  - use of a code transmitted by the Bank via SMS to the Cardholder's mobile phone number registered with the Bank;
  - use of a code determined with the card inserted in a chip reader expressly approved by the Bank together with the PIN; or
  - other codes generated by identification tools expressly approved by the Bank.
- verification via card details and personal information

Identification may occur on individual security levels or a combination thereof. The Bank reserves the right to modify identification procedures and features for accessing and individual services for electronic functionalities.

4. Legitimation
The Bank deems as authorized any access to or use of the electronic functionalities by anyone if at the time of said use legitimation has occurred in compliance with applicable security provisions as set forth in 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 differing provisions set forth in forms issued by the Bank (card applications, etc.). The Bank reserves the right, however, to deny access to the electronic functionalities at any time and without providing reasons.

5. Security; obligations of due diligence
The Cardholder is 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.

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. Availability, liability
The Bank will make every effort to maintain the electronic functionalities uninterrupted, but can guarantee neither unlimited access to nor unlimited use of all of its functionalities. Also, the Bank cannot guarantee unlimited operating capability on the part of telecommunication networks.

The Bank reserves the right to suspend access to and usage of the electronic functionalities at any time and without notice, in particular for the purpose of carrying out maintenance operations. Subject to any limitations arising from the legal provisions in force, the Bank is not liable for any direct or indirect damages caused to the Cardholder or to third parties as a result of access to and/or use of, or inability to access or use, the services for electronic functionalities. In particular, the Bank is not liable for damages which arise as a consequence of mistakes during the transmission or processing of data, or as a consequence of defects, interruptions, malfunctions, interceptions, or service suspensions. The Bank also is not liable for damages arising from mistakes in data transmission, late processing, or the provision of card data on public networks (the Internet).

7. Charges
Charges for electronic functionalities which are liable to pay costs, are billed directly on the monthly statement. Applicable usage charges are listed on the Bank's website. Roaming charges may apply when the electronic functionalities are used outside Switzerland.

8. Contract amendment
The Bank reserves the right to amend these Conditions of Use at any time. The Cardholder will be notified of such changes by circular letter or in some other appropriate form. The changes will be regarded as accepted if the Cardholder raises no objection in writing within 30 days of notification.

9. Activation, duration, and other conditions
The Cardholder may apply for access to, activate, or cancel the services for electronic functionalities at any time. Unless otherwise stated in these Conditions, the Cardholder's access to the services for electronic functionalities will remain active until the expiration of the Cardholder's valid card. These Conditions replace all prior Conditions of Use governing the same matters. The General Terms and Conditions for the Diners Club Cards of Cornèr Bank Ltd. apply in full to any matter not covered by these Conditions of Use.

Version 08.2017

Cornèr Banca SA, Cornèrcard,
Via Canova 16, 6901 Lugano, Tel: +41 58 880 88 00, dinersclub.ch