Conditions of Use of One Services

Article 1 - Conditions of use of One Services

1.1 Conditions of use of One Services and other relevant documents

These conditions of use apply to the online services designated by the term 'One' (hereinafter '**One Services**') and provided by Banque Cantonale de Genève (hereinafter the '**bank**') to holders (hereinafter the '**cardholders**') of a Debit Mastercard (hereinafter the '**card**').

Viseca Payment Services SA (hereinafter the '**subcontractor**') acts as a subcontractor in the provision of One Services. The cardholder authorises the bank to provide the subcontractor with data concerning the cardholder, the card and the account(s) to which the card is attached. **For the purposes of these communications, the cardholder releases the bank from the obligation to comply with banking and professional secrecy (Art. 47 of the Federal Banking Act and similar provisions).**

One Services can be accessed via:

- the 'one' website (the '**website**'); and
- the 'one' application (the '**application**').

Additional information on the processing of cardholders' personal data can be found in the bank's Data Privacy Notice (bcge.ch/en/protection-des-donnees), the current version of which may be consulted using the link above and obtained from the bank (hereinafter the 'BCGE Data Privacy Notice').

These conditions of use are applicable in addition to the conditions of use of the Debit Mastercard (available at bcge.ch/en/dmc), the current version of which can be consulted using the link above and obtained from the bank (hereinafter 'conditions of use of the DMC'). In the event of any contradiction, these conditions of use shall prevail over the conditions of use of the DMC.

1.2 What are One Services?

One Services comprises the services of the bank, provided by the subcontractor on behalf of the bank. The use of One Services requires prior registration. Newly introduced One Services are made available to cardholders by means of updates. The bank shall inform the cardholders of developments and, where applicable, of the related amendments to these conditions of use.

1.3 What functions do the One Services offer?

The One Services may - now or in the future - include in particular the following functions:

- User account for the administration of personal data in connection with the cards;
- Control and confirmation of payments, for example using '3-D Secure' technology (Mastercard SecureCode) with the application or by entering an SMS code (refer to section 5);
- Control and confirmation of certain operations (e.g. logins, communications exchanged with the bank) with the application or by entering an SMS code;
- Activation of cards for the use of means of payment;
- Exchanges of messages and notifications of all kinds between the cardholder and the bank, subject to cases in which a particular form of notification is required (e.g. a written challenge to an account statement);
- Overview of transactions or cards;
- Overview of the bonus programme account and the possibility of using points;
- Information relating to the use of the card.
- Overview of information relating to the account(s) to which the card is attached.

Article 2 - Use of One Services

2.1 Right of use

The cardholder is only authorised to use the One Services if he is able to implement these conditions of use and the related requirements (in particular section 3.2).

2.2 Processing of personal data within the framework of One Services

By using One Services, the cardholder acknowledges that the bank (and the subcontractor) undertakes the processing of personal data listed below (in addition to those listed in the BCGE Data Privacy Notice); this processing is based on the execution of the contract concluded between the bank and the cardholder within the framework of One Services:

- Processing of personal data which is or will be collected when using One Services (i.e. the identification data of the cardholder, the data relating to the account to which the card is attached and the transactions carried out using the card and/or One Services).
- Electronic communication by e-mail (using the e-mail address provided during registration) as well as through the application (e.g. notification of changes of address, notification of changes to the conditions of use or notifications related to the fight against fraudulent use of cards).

Furthermore, the cardholder acknowledges that the bank (respectively the subcontractor if the processing is delegated) undertakes the following processing of personal data, based on the legitimate interest of the bank to the promotion of its products and services:

- Receipt of messages and information concerning bank products and services for marketing (advertising) purposes. These messages may be distributed by the bank via e-mail or directly in the application or on the website. This processing of personal data includes in particular the linking by the bank of data collected as part of the One Services with already existing data deriving from the client-relationship in order to conduct profiling for marketing purposes (but also for risk management purposes).

The cardholder may at any time indicate to the bank that he does not want the bank to process personal data concerning him with a view to offering products and services and/or for other marketing purposes (right to 'opt out'). Any such indication must be communicated to the bank using the contact details found in the BCGE Data Privacy Notice (bcge.ch/en/protection-des-donnees).

2.3 Refusal or withdrawal of consent by the cardholder

If the cardholder refuses the processing referred to in section 2.2 (with the exception of processing for marketing purposes/third point in section 2.2 above), the application or the website or some of their individual services may not or no longer be used, depending on the circumstances.

2.4 Consequences of confirmations

Each confirmation made by means of the application or by entering an SMS code is considered as an operation carried out by the cardholder. The cardholder undertakes to pay the card debits resulting from these confirmations and irrevocably authorises the bank to carry out the respective orders and procedures.

2.5 Availability/blocking/modifications

The bank may at any time (and even without advance notice) totally or partially interrupt, limit, suspend or replace the One Services with another service. In particular, the bank has the right to temporarily or permanently block the cardholder's access to One Services (for example, in the event of suspected abuse).

2.6 Intellectual property rights and licence

All rights (in particular copyright and trademark) on software, texts, images, videos, names, logos and other data and information, accessible, now or in the future, via the One Services, belong exclusively to the bank or to the respective partners and third parties (e.g. the subcontractor). The names and logos visible as part of One Services are protected trademarks.

The Bank grants the cardholder a non-exclusive, non-transferable, open-ended, revocable at any time and free licence to download the application, install it on a device that the cardholder permanently owns and use it in accordance with these conditions of use.

Article 3 - Risks, exclusion of guarantee and general due diligence and communication obligations

3.1 Risks when using One Services

The cardholder acknowledges and accepts that the use of One Services involves risks.

In particular, it is possible that when using One Services, unauthorised third parties may fraudulently use the card(s), the username and password, the devices used or the personal data of the cardholder (or persons linked to the cardholder). In doing so, the cardholder may suffer financial loss (e.g. if his account is then unduly debited for fraudulent use of the card or the application) and a violation of his personal rights (e.g. in the event of misuse of his personal data). In addition, there is a risk that One Services or one of the services offered as part of One Services cannot be used.

Abuses are made possible or facilitated in particular by:

- the violation by the cardholder of the obligations of due diligence or communication (see section 3.2) (e.g. during the negligent handling of his username/password or failure to report a loss of the card);
- the settings selected by the cardholder or the lack of maintenance of the devices and systems used for the use of One Services (e.g. computers, mobile phones, tablets and other IT infrastructure), for example by the absence of a screen lock, by the absence or insufficiency of a firewall or anti-virus protection or by the use of an outdated software;
- interventions by third parties or errors in the transmission of data over the internet (such as hacking, phishing or loss of data);
- incorrect confirmations in the application or by the insertion of an SMS code (e.g. in the event of insufficient verification by the cardholder of a confirmation request);
- the selection by the cardholder of weak security settings for One Services, in particular when using the application (e.g. saving the login).

If the cardholder complies with his due diligence obligations when using the devices and the password as well as the verification obligations for confirmation requests, he can reduce these risks of misuse. Further information on risk reduction when using One Services is available on the website https://one.viseca.ch/login/login?lang=en.

The bank does not provide any guarantee and does not give any assurance that the website and the application will be permanently accessible or operate without interruption or that abuses can be recognised and avoided with certainty.

3.2 General due diligence obligations of the cardholder

3.2.1 General due diligence obligations relating to the devices and systems used, in particular mobile devices

One Services allows, in particular, the authentication of the cardholder through the cardholder's mobile device (e.g. mobile phone, tablet; hereinafter '**mobile device**'). The careful storage of these mobile devices by the cardholder at all times is an essential security factor. The cardholder must use mobile devices with appropriate care and ensure their adequate protection.

Furthermore, the cardholder is required to comply in particular with the following due diligence obligations in connection with the use of devices and systems, in particular mobile devices:

- For mobile devices, the cardholder must activate a screen lock and take other security measures to prevent unlocking by unauthorised third parties;
- Mobile devices must be kept in a secure place so as to be protected from third-party access, and must not be handed over to third parties for permanent or uncontrolled use;
- Software (e.g. operating systems and internet browser) must be regularly updated;
- Interference in operating systems (e.g. 'Jailbreaking' or 'Rooting') is prohibited;
- Anti-virus protection and 'Internet Security' type software must be installed on computers/laptops and updated regularly;
- The application must be downloaded exclusively from the official stores (e.g. Apple Store and Google Play Store);
- The updates of the application must be installed immediately;
- If a mobile device is lost, all possible measures must be taken to prevent unauthorised third-party access to the data transferred to the mobile device (e.g. by blocking the SIM card, by blocking the device, by deleting the data remotely using 'Find My iPhone' or 'Android Device Manager', by resetting or having the user account reset). Any loss of a mobile device must be reported to the bank (see section 3.3);
- The application must be deleted prior to a sale or other permanent transfer of the mobile device to a third party.

3.2.2 General due diligence obligations relating to the password

In addition to possession of the mobile device, the username and password serve as additional elements for the authentication of the cardholder.

The cardholder is required to comply with the following due diligence obligations in relation to the password:

- the cardholder must choose a password which is not already used for other services and which must not consist of easily decipherable combinations (such as telephone numbers, dates of birth, licence plates, names of the cardholder or relatives, sequences of numbers or letters that are repeated or that follow each other directly such as '123456' or 'aabbcc');
- the password must be kept confidential. It must not be disclosed or made accessible to third parties. The cardholder acknowledges that the bank will never ask him to disclose his password;
- The password should not be written down or saved in an insecure manner;
- The cardholder must change the password or reset the user account or have it reset by the bank if there is a suspicion that a third party has knowledge of the password or taken possession of other data;

- The password must only be entered in such a way that it is not visible to third parties.

3.2.3 General due diligence obligations relating to confirmation requests

Confirmations are legally binding on the cardholder.

Therefore, the cardholder is required to comply with the following general due diligence obligations relating to confirmations in the application or by entering the SMS code:

- The cardholder must only confirm if the confirmation request is directly linked to a specific transaction or action of the cardholder (e.g. payment, login or contact with the bank);
- Before confirming, the cardholder must verify whether the subject of the confirmation request corresponds to the action concerned. If requesting confirmation in connection with '3-D Secure' technology, the cardholder must check the payment details displayed.

3.3 General obligations of the cardholder to communicate

The following events must be reported to the bank immediately (whose contact details are available on bcge.ch):

- Loss of a mobile device, but not a short-term loss;
- A suspicion of misuse, for example, in connection with the receipt by the cardholder of a request for confirmation that is not related to a transaction carried out by the cardholder (online payment, login, contact with the bank or other similar processes);
- Any other suspicion that a confirmation request in the application or an SMS code does not come from the bank;
- Case of suspected abuse, in particular of the username, password, mobile devices, website, application, or suspicion that an unauthorised third party has come into possession of this information or objects;
- Change of telephone number and other relevant personal data;
- Change of the mobile device that is used for One Services (in this case, the application must be registered again).

Article 4 - Liability

It is the responsibility of the cardholder to implement due diligence obligations in order to prevent unauthorised use of One Services. It is the responsibility of the cardholder to take appropriate measures to prevent the risk of fraud in the use of One Services. The cardholder shall bear any damage resulting from the violation of his due diligence obligations.

Furthermore, damages resulting from lack of legitimacy or undetected fraud are the responsibility of the cardholder, except in the event of gross negligence by the bank.

Article 5 - 3-D Secure

5.1 What is 3-D Secure?

3-D Secure (called 'Secure Code' in the context of the Mastercard payment system) is an internationally recognised security standard for online card payments. The cardholder is required to use this security standard when making payments, insofar as it is offered by the point of acceptance (retailer).

The use of 3-D Secure is only possible after registering with One Services.

5.2 How does 3-D Secure work?

Payments made using 3-D Secure can be confirmed (authorised) in two ways:

- in the application or,
- by entering the code that the bank sends to the cardholder by message (SMS code) in the corresponding browser window during the payment process.

In accordance with the conditions of use of the DMC (available at bcge.ch/en/dmc), each use of the card authorised via 3-D Secure technology is deemed to have been carried out by the cardholder.

5.3 Card activation for 3-D Secure

When registering with One Services, 3-D Secure technology is activated for all cards in the name of the cardholder that are related to the business relationship between the cardholder and the bank.

5.4 Deactivation of 3-D Secure

For security reasons, 3-D Secure cannot be deactivated after activation.