Conditions governing the use of one Digital Services

As at June 2021

A) one Digital Services

1 Conditions of use

These conditions apply to holders (hereinafter referred to as "Authorised Card Holder") of a debit card (hereinafter referred to as "card"). They comprise online services (hereinafter referred to as "services") that are provided by Zuger Kantonalbank (hereinafter referred to as "Bank") under the name one. one is managed by Viseca Card Services SA (hereinafter referred to as "Processor). The Bank involves the Processor in the performance of its duties arising from the card business. one is available via the one website and the one app.

The further conditions pertaining to one – in particular regarding the processing of data and data security – in the Bank's data privacy statement, the data privacy conditions and conditions of use of the Processor for one and the conditions of use of the website itself have to be taken into consideration. The Bank's General Terms and Conditions also apply.

These conditions apply in addition to the conditions for the use of the debit card. Where there are deviations, these conditions take precedence over the conditions for the use of the card.

2 Scope of functions

Either at present or in future, one may comprise the following functions in particular:

a) User account for the management of personal data
b) Checking and confirmation of payments, e.g. by way of 3-D Secure (Verified by Visa) in the app or by entering an SMS code (see section B "3-D Secure")
c) Checking and confirmation of specific actions (e.g. logins, contacting the Bank) in the app or by entering an SMS code
d) Activation of cards in order to use specific payment options (see section C "Mobile payment")
e) Exchange of notices and messages between the Authorised Card Holder and the Bank in relation to the card and one (e.g. notifying a change in the conditions), except where a special form of notification or message is reserved (e.g. written objection to a monthly invoice)
f) Overview of transactions or cards and electronic display of invoices
g) Information concerning the use of the card

3 Usage authorisation

The Authorised Card Holder is only authorised to use one under the following conditions:

a) They are able to comply with these conditions and the related requirements (in particular section 5a–5c)
b) They are authorised to use a debit card of the Bank as the holder.

4 Effect of confirmations

Each confirmation given via the app or by entering an SMS code is deemed to be an action by the Authorised Card Holder. The Authorised Card Holder and the account holder, if not identical to the Authorised Card Holder, undertake to accept responsibility for charges to the card made on the strength of confirmations and authorise the Bank to execute related orders and engage in related actions (in particular to debit the account).

5 Due diligence obligations of Authorised Card Holder

a) Devices and systems used

For authentication, one uses mobile devices, among others (e.g. mobile phone, tablet) of the Authorised Card Holder. It is therefore essential for security purposes that these mobile devices are always in the custody of the Authorised Card Holder. The Authorised Card Holder must therefore specifically comply with the following due diligence obligations in relation to the devices and systems that are used, in particular the mobile devices:

i. For mobile devices, a screen lock must be activated and further security measures implemented to prevent the unlocking of the device by unauthorised persons
ii. Mobile devices must be protected against third-party access and kept in a safe place, and may not be given to third parties for permanent or unsupervised use
iii. Software (e.g. operating systems and internet browsers) must be regularly updated
iv. Operating systems may not be interfered with (e.g. jailbreaking or rooting)
v. Virus protection and internet security programs must be installed and kept up to date on laptops/computers or mobile devices
vi. The app may only be downloaded from the official stores (e.g. Apple Store and Google Play Store)
vii. Updates to the app must be installed immediately
viii. If a mobile device is lost, everything possible must be done to prevent unauthorised persons from accessing the data sent to the mobile device by the Bank (e.g. blocking the SIM card, blocking the device, erasing the data, e.g. via Find My iPhone or Android Device Manager, resetting or requesting a reset of the user account). The Bank must be informed of the loss (see section 6)
ix. The app must be deleted before selling or otherwise permanently passing on the mobile device to a third party

b) Password

In addition to having actual custody of the mobile device, the user name and password serve as additional factors for identifying the Authorised Card Holder. With regard to the password, the Authorised Card Holder must comply with the following due diligence obligations in particular:

i. The Authorised Card Holder must set a password which does not contain combinations that are easy to guess (e.g. telephone number, date of birth, car registration number, name of Authorised Card Holder or persons close to them, repeated or direct sequences of numbers or letters such as

"123456" or "aabbcc") and is not already used for other services.

ii. The password must be kept secret. It may not be disclosed or made accessible to third parties. The Authorised Card Holder acknowledges that the Bank will never ask the Authorised Card Holder to disclose their password

iii. The password may not be written down or stored in an unsecured manner

iv. The Authorised Card Holder must change the password or reset the user account or request the Bank to reset the account if there is reason to suspect that a third party has obtained access to the password or other data.

v. Care must be taken when entering the password that it cannot be viewed by third parties

c) Requests for confirmation

Confirmations confer a binding obligation on the Authorised Card Holder. The Authorised Card Holder must therefore comply with the following due diligence obligations in relation to confirmations provided in the app or by entering an SMS code:

i. The Authorised Card Holder may only enter a confirmation if the request for a confirmation is directly related to a specific action or process (e.g. payment, login, contact with the Bank) executed by the Authorised Card Holder

ii. The Authorised Card Holder must check before giving the confirmation that the confirmation request matches the specific process. In particular, the payment details shown in requests for confirmation relating to 3-D Secure must be checked

6 Notification obligations of Authorised Card Holder

The Bank must be informed of the following events immediately:

a) Loss of a mobile device, but not the temporary misplacement of the device

b) Requests for confirmation that are not related to an online payment, a login attempt by the Authorised Card Holder, the establishment of contact with the Bank or similar processes (suspected misuse)

c) Any suspicion that requests for confirmation in the app or the SMS code do not come from the Bank

d) Suspicion of misuse of user names, passwords, mobile devices, the website, the app, etc., or a suspicion that unauthorised third parties have obtained possession of such

e) Changes to telephone numbers and other relevant personal data

f) Replacement of the mobile device that is used for one (in which case the app must be registered again)

The Bank must be immediately informed by telephone of suspected misuse or the loss of a mobile device: +41 (0)41 709 11 11

7 Liability

a) General liability for damage

Subject to section 7 b), the Bank shall provide indemnity for any damage that is not covered by an insurance policy

i. if the damage in question was caused by demonstrably illegal interference in systems of network and/or telecommunication operators or in the devices and/or systems used by the Authorised Card Holder (e.g. computer, mobile devices and other IT infrastructure) and provided that the Authorised Card Holder complied with the special due diligence and notification obligations set out in sections 5 and 6 above, in particular the obligation to check requests for confirmation and the obligation to check the monthly invoice pursuant to the conditions for using the card as well as timely objection to abusive transactions, and provided also that the Authorised Card Holder is not in any other way responsible for the damage

ii. if the damage in question was caused exclusively by the violation of the Bank's normal commercial due diligence obligations

Unless caused intentionally or through gross negligence on its part, the Bank shall not accept any liability for indirect or consequential damage of any kind suffered by the Authorised Card Holder.

b) Exceptions

In the following cases the Authorised Card Holder shall bear responsibility for damage and the Bank shall not accept any liability:

i. if, pursuant to section 7 a), the Bank does not provide indemnity for the damage in question (in particular in the event of a breach by the Authorised Card Holder of their due diligence and notification obligations)

ii. if the Authorised Card Holder, their partner, direct family members (in particular children and parents) or other persons closely related to the Authorised Card Holder, authorised representatives and/or persons living in the same household carried out an action (e.g. confirmation in the app or via SMS code)

8 Consent provided upon registration and relating to the further development of one

By using one, the Authorised Card Holder expressly grants the Bank the following permissions:

a) Consent to the processing of data that is or was collected through the use of one. This specifically includes consent to the linking of such data with data already held by the Bank and the preparation of profiles, in particular for the purposes of risk management and marketing by the Bank or the Processor and third parties in accordance with the one data privacy statement

b) Consent to being sent messages and information about products and services of the Bank and third parties for marketing purposes (advertising). The Bank and third parties can deliver these by e-mail or directly in the app or on the website.

c) Consent to the use of the e-mail address provided upon registration as well as the website and the app for the exchange of electronic communication with the Bank, but only in connection with the card and one (e.g. notice of amendments to these conditions or notices relating to the combating of card misuse)

9 Refusal of consent relating to the further development of one

If the Authorised Card Holder does not consent to the conditions relating to the further development of one (e.g. updates), it may be or become impossible to use the app or the website or some of their services.

10 Availability/blocking/changes

The Bank may at any time, in whole or in part, interrupt, restrict or discontinue the use of one or replace it by another service, possibly also without giving prior notice.

The Bank in particular has the right to temporarily or permanently block the Authorised Card Holder's access to one (e.g. if misuse is suspected).

11 Intellectual property rights and licence

Unless stated otherwise in these conditions, all rights (in particular copyrights and trademark rights) to software, texts, images, videos, names, logos and other data and information that are accessible via one or become accessible in the course of time belong exclusively to the Bank or the relevant partners and third parties (e.g. Processor, Visa). The names and logos that can be seen in one are protected trademarks.

The Bank grants the Authorised Card Holder a non-exclusive, non-transferable, unlimited, revocable and free licence to download the app, to install it on one (or more) device(s) in the permanent custody of the Authorised User and to use it within the parameters of the intended functions.

Use of the website is subject also to the licence provisions set out in the conditions of use of the website (in the section "Ownership of website, trademarks and copyrights").

12 Risks associated with the use of one

The Authorised Card Holder acknowledges and accepts that the use of one entails certain risks. It is in particular possible that using one can lead to the misuse by unauthorised third parties of cards, user names and passwords, devices or personal data of the Authorised Card Holder. This can cause the Authorised Card Holder financial damage (charges to the card) as well as personal damage (misuse of personal data). There is also a risk that one or a service offered on one cannot be used (e.g. logging in to one may not be possible).

Specifically, misuse may be facilitated or promoted by:

- violation by the Authorised Card Holder of due diligence or notification obligations (e.g. careless handling of user name/password or failure to notify the loss of the card)
- the settings chosen by the Authorised Card Holder or insufficient maintenance of the devices and systems used for one (e.g. computer, mobile telephone, tablet and other IT infrastructure), e.g. missing screen lock, missing or insufficient firewall or virus protection, or outdated software
- interference by third parties or errors in the transmission of data via the internet (e.g. hacking, phishing or loss of data)
- erroneous confirmations in the app or entry of an SMS code (e.g. failure to check a request for confirmation)
- weak security settings chosen by the Authorised Card Holder for one – in particular for the app (e.g. saved login data)

The Authorised Card Holder can reduce the risks of misuse by complying with the due diligence and notification obligations set forth in these conditions for using mobile devices and passwords as well as the obligations to check requests for confirmation. Further information about minimising the risks associated with the use of one is provided on the website.

The Bank does not warrant and does not provide any guarantees that the website and the app will always be accessible or be free of malfunction or that misuse will be recognised and definitely prevented.

B) 3-D Secure

13 Conditions of use

Pursuant to the Bank's conditions for using the card, the Authorised Card Holder is obliged to use this security standard for payments, provided that it is offered by the accepting merchant. 3-D Secure can only be used after registration with one.

14 Authorisation

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

a) in the app
b) by entering a code sent by text message by the Bank to the Authorised Card Holder (SMS code) into the applicable browser window during the payment transaction

Pursuant to the Bank's conditions for using the card, each authorised use of the card with 3-D Secure is deemed to have been made and accepted by the Authorised Card Holder.

15 Activation of card for 3-D Secure

By registering on one, 3-D Secure is activated for all cards issued in the name of the Authorised Card Holder and pertaining to the registered business relationship between the Authorised Card Holder and the Bank.

16 Deactivation of card for 3-D Secure

For reasons of security, 3-D Secure cannot be deactivated once it has been activated.

C) Mobile payment

17 How it works

"Mobile payment" refers to solutions for using cards via a mobile device. It enables Authorised Card Holders with a compatible mobile device to use authorised cards via a mobile application (app) of the Bank (see section 23) or a third party for contactless payment and for payment in online shops and apps. For security reasons, a number that is different from the card number (token) is generated and stored as a "virtual card". Virtual cards can be used via mobile payment in the same way as a physical card. When payment is made with a virtual card, only the generated number ("token") and not the actual card number is passed to the merchant.

18 Availability

Mobile devices such as computers, mobile phones, smart watches and fitness trackers are compatible if they support the use of virtual cards and are accepted by the Bank. The Bank decides at its discretion which cards it accepts for which providers.

19 Activation and deactivation

For security reasons, a card can only be activated if the Authorised Card Holder accepts the conditions of use and acknowledges the data privacy statement of the relevant provider.

Virtual cards can be used via the app by the Authorised Card Holder until the card is blocked or deactivated, subject to the restrictions on the use of the card as set forth in the Bank's currently applicable conditions of use for the card.

The Authorised Card User can terminate the use of mobile payment at any time by deleting their virtual card(s) with the relevant provider.

Costs pertaining to the activation and use of virtual cards (e.g. mobile internet costs abroad) shall be borne by the Authorised Card Holder.

20 Authorisation
A virtual card is used in the same way as a customary card transaction. Each instance of using a virtual card is deemed to have been authorised by the Authorised Card Holder.

The use of virtual cards must be authorised in the manner prescribed by the provider or merchant, e.g. by entering a device PIN or by fingerprint or face recognition. The Authorised Card Holder notes that the risk that virtual cards can be used by unauthorised persons is increased if the means of authorisation (device PIN or card PIN) prescribed by the provider or merchant consists of combinations that are easy to guess ("1234"). The Authorised Card Holder notes that the provider or merchant can decide to forgo authorisation up to an amount to be determined by them. In all other respects, liability is governed by section 7 of these conditions.

21 Special due diligence obligations
The Authorised Card Holder acknowledges and accepts that, in spite of all the security measures taken, the use of mobile payment entails certain risks. In particular, it is possible that virtual card(s) and personal data may be misused or viewed by unauthorised persons. This may cause the Authorised Card Holder financial damage (fraudulent charges on a card) as well as personal damage (misuse of personal data).

The Authorised Card Holder must therefore treat the devices and virtual cards with due care and ensure their protection. In addition to the due diligence obligations pursuant to the Bank's applicable conditions for using the card and the general due diligence and notification obligations pursuant to sections 5 and 6, the Authorised Card Holder must comply with the following special due diligence obligations in particular:

a) The devices must be used in accordance with instructions and be kept in a safe place where they are protected against access by third parties.
b) Like physical cards, virtual cards are personal and non-transferable. They may not be made available for use by third parties (e.g. by storing the fingerprints or scanning the face of a third party to unlock the device).
c) If a mobile device is replaced or passed on to another person (e.g. when sold), each virtual card in the provider's app and the mobile device must be deleted.
d) The Bank must be informed immediately of any suspected misuse of a virtual card or a device used for this purpose to ensure that the virtual card in question can be blocked.

22 Warranty exclusion
There is no entitlement to the use of mobile payment. The Bank may at any time interrupt or terminate the use of mobile payment, i.e. the option to use virtual cards, in particular for reasons of security or if the mobile payment offering is modified or if the authorised cards or compatible devices/versions are subjected to restrictions.

Furthermore, the Bank is not responsible for actions and offers of the provider or other third parties such as providers of internet and telephony services.

23 Use of card via one app
Authorised Card Holders with a compatible device can activate and use their card(s) as a virtual card in the one app. To ensure mobile payment security, the Authorised Card Holder must set a secret number upon activation. The Bank may adjust this service at any time. In all other respects, the conditions for mobile payment and in particular the special due diligence obligations pursuant to section 21 shall apply.

24 Data privacy
The third party provider and the Bank are independently responsible for their own processing of personal data. The Authorised Card Holder acknowledges that personal data is collected by third-party providers in connection with the offer and use of mobile payment (in particular data relating to the holder and activated cards and transaction data concerning the use of virtual cards) and is stored and processed further in Switzerland or abroad. The processing of personal data by the third-party provider in relation to mobile payment and the use of the third-party provider's offers and services as well as its devices and software are governed by its conditions of use and data privacy provisions. The Authorised Card Holder therefore confirms with each activation of a card that they have read and understood the relevant data privacy provisions of the third-party provider in question and that they explicitly agree to the processing of their data by the third-party provider. If the Authorised Card Holder does not agree to this processing, they must refrain from activating their card or object to the processing of their data by the third-party provider. The processing of personal data by the Bank and the Processor is subject to the data privacy statements of the Bank and of one.

Effecitve as of 7th June 2021