CREDIT SUISSE

Terms and conditions for use of mobile payment solutions

1. Applicability/overview of services
These terms and conditions for use apply when a debit card or a means of payment serving the same purpose (**"Card"**) from Credit Suisse AG or Credit Suisse (Switzerland) Ltd. (**"Bank"**) is electronically stored and used in a mobile payment solution (**"Mobile Wallet(s**)").

The terms and conditions of use are considered accepted as soon as the client has registered via the Mobile Wallet (see point 2).

The contractual terms and conditions of the provider in question (**"Provider(s)"**) apply to the Mobile Wallet, the device on which the Mobile Wallet will be used, and, where applicable, the digital accounts used by the Bank client and anyone authorized by the client to use the Card, e.g. a partner card (**"User(s)"**). The Bank is not the Provider of the mobile payment solution; rather, it simply facilitates Users storing their Cards in the Mobile Wallet of the Provider as a means of payment. The Bank has no influence on the functionality, availability, or scope of the Mobile Wallet functions; the Provider can change such features pursuant to its own contractual terms and conditions. This applies likewise to the Provider's option to restrict and/or temporarily or permanently suspend use of the Mobile Wallet. Claims against the Bank in relation to Mobile Wallet functionality are therefore excluded in all instances.

These terms and conditions for use apply in addition to the other applicable provisions governing the contractual relationship between the Bank and the User(s), including in particular the relevant General Conditions of the Bank and the Conditions Governing the Use of Debit Cards (both available at: www.credit-suisse.com/ch/en/legal.html). In the event of conflicting provisions, these terms and conditions for use will take precedence over any other contractual terms and conditions of the Bank.

The Bank reserves the right to amend these terms and conditions for use at any time. Users will be made aware of changes in a suitable format and such changes will be considered accepted provided the User has a Card registered pursuant to point 2 at the time when the change enters into force.

2. Registration
A Mobile Wallet can only be used for cashless payments via Card ("Mobile Wallet Transaction") once the Card in question has been registered in the respective Mobile Wallet.

To register a Card, the User will be asked to enter the name printed on the Card, the Card number, the expiration date, the Card verification value/code (CVV, CVC), and any other data that may be requested by the Mobile Wallet operator (**"Card Data"**). This Card Data must be entered manually, if appropriate by scanning it in using a camera or an alternative method of automatic Card Data read-in, e.g. via an app (known as in-app provisioning), or by other means, in accordance with the Mobile Wallet operator's regulations. Once all the Card Data has been entered, various checks are carried out by the global card network, e.g. Mastercard (**"Card Network Company"**), the Mobile Wallet operator, the Bank, or the Bank's service providers.

Once these checks are complete, additional steps can be taken to authenticate the User. Successful registration will be confirmed to the User by the Bank either directly in the Mobile Wallet, by SMS, or by other means. The Bank is entitled to deny Card registration without stating reasons.

Once the Card has been successfully registered, a digital Card number will be generated (**"Digital Card Number"**) and stored in the Mobile Wallet (**"Electronic Storage"**).

3. Mobile Wallet Transaction and transaction approval
A Mobile Wallet can be used by the client as a means of payment in physical stores, at vending machines, in online stores, and in apps operated by merchants or service providers who accept the Mobile Wallet as a means of payment (**"Merchant(s)"**).

The manner in which and the time frame within which a transaction is approved (e.g. by entering a PIN or through biometric data such as fingerprint scan or facial recognition, or by simply using the device) is determined by the Provider's specifications.

The client is aware and acknowledges that any person confirming their identity by accessing the device and using the Mobile Wallet (e.g. by entering the relevant code), and/or confirming a transaction via the device, and setting up the Mobile Wallet as a means of payment with Merchants, or using the Mobile Wallet in any other way is considered by the Bank to be authorized to complete transactions using the Mobile Wallet. This applies even if the person in question is not the actual owner of the device.

4. Client's obligation to exercise due care
When using the Mobile Wallet, the client must observe the following due diligence obligations:

a. Users must take the necessary measures (e.g. device or screen lock) to prevent the unauthorized use or manipulation of their device.
b. Users must keep their personal means of identification secret. They may not disclose their means of identification to third parties. Means of identification from third parties (e.g. biometric data for a third party, such as a fingerprint) for unblocking must not be stored on or with the respective device or in the Mobile Wallet.
c. If there is reason to believe that unauthorized persons have gained access to the device or screen lock, the means of identification for the device or screen lock must be changed immediately.
d. Users must report the loss or even simply the suspected loss of the device immediately, in particular in the event of theft, so that the Digital Card Number can be blocked. In addition, Users must immediately block the SIM card (or have it blocked by the network operator) and, if possible, also have the device blocked by the device manufacturer.
e. Turning off the security features by installing unofficial apps or operating systems (jailbreaking) or similar manipulations of the device (e.g. setting up root access – i.e. access at the device system level) or by installing apps that are not permitted by the provider of the operating system (because, for example, they make the device more susceptible to viruses and malware) is prohibited. Any manipulation of the device is carried out at the risk and responsibility of Users; the Bank accepts no liability for damage resulting from or in connection with such manipulation.
f. The client is obligated to delete all Card and transaction data from the device prior to (temporarily or permanently) handing over the device to a third party (e.g. sale, gift, loan, deposit, pawn, repair).
g. The due diligence and cooperation obligations pursuant to the Conditions Governing the Use of Debit Cards as well as the contractual terms and conditions of the Mobile Wallet operator to which Users are subject also apply.
h.

The User or the Bank client accepts liability for all risks and consequences arising from the use – including the fraudulent use – of a Mobile Wallet (e.g. by unauthorized persons or for unauthorized purposes). Acceptance of liability for damages pursuant to the Conditions Governing the Use of Debit Cards is reserved.

5. Changes to the Card or Electronic Storage

Any renewal, termination, blocking, or unblocking of the Card also affects its use via the Mobile Wallet.

Electronic Storage can be terminated, blocked, or unblocked separately for each device, independently of the physically issued card and without changing the Card status; however, in contrast to the provisions outlined for cards in the Conditions Governing the Use of Debit Cards, this process must be carried out separately for each Card by the respective owner of the Mobile Wallet. Payments initiated before the block was in place are considered booked and cannot be reversed.

Users can, if provided for by the Mobile Wallet operator, terminate Electronic Storage in accordance with the regulations and instructions of the Mobile Wallet operator (e.g. by removing the Card-related data from the Mobile Wallet). Users can, if provided for by the device manufacturer, also terminate Electronic Storage by deleting the Mobile Wallet from the device or by resetting the device to the factory settings (deleting all data entered by the User).

The Bank reserves the right to terminate or restrict Electronic Storage for specific Mobile Wallets or all Mobile Wallets in full or in part at any time without stating reasons.

6. Fees

Cardholders are solely responsible for the availability of compatible devices that support the use of the Mobile Wallet.

All costs, fees, and expenses charged by the Provider for mobile telephony and/or telecommunications services in connection with the installation and/or use of the Mobile Wallet will be borne by the User or the Bank client.

7. Data protection

The processing of information pertaining to Users, in particular client data, Card Data, and transaction data as well as the Digital Card Number (**"Client Data"**) is always carried out pursuant to the Bank's privacy statement, which is available at: www.credit-suisse.com/ch/en/legal.html).

During registration and use, additional device information, data from a SIM card or memory card, and geo data (**"Device Data"**) as well as information relating to the business relationship of the User with the Mobile Wallet operator (including in its capacity as device manufacturer or operator of an operating system installed on the device, [**"Mobile Wallet Operator Data"**]) may also be processed for the purposes described in these terms and conditions for use.

Within the scope of the registration, renewal, termination, blocking, and unblocking of Electronic Storage and/or Mobile Wallet Transactions, Client Data, and Device Data as well as Mobile Wallet Operator Data may be exchanged between the Bank, the Mobile Wallet operator, and Card Network Company for the following purposes:

- Checking whether Electronic Storage is permitted.
- Verifying and reconciling the identity of the User and the device owner.
- Preventing and investigating misuse and fraud.
- Complying with supervisory regulations (e.g. national/international sanctions).
- Creating or updating the Digital Card Number and reconciling status information (renewal, termination, blocking, unblocking, etc.) between the Card and Electronic Storage.
- Creating a list in the Mobile Wallet of past transactions (e.g. information about the acceptance point, transaction amount, and transaction date).

The contractual terms and conditions of the Mobile Wallet operator may stipulate that the data mentioned in this section can be acquired, processed, and disclosed by the Mobile Wallet operator (including any third parties) for further purposes. The Bank is not responsible for the acquisition, processing, and disclosure of data by the Mobile Wallet operator, the Card Network Company, or any third parties commissioned by them. This is regulated by their contractual terms and conditions.

8. Data transfer and electronic communication

Users acknowledge that Mobile Wallet operators, Card Network Companies, acceptance points, and third parties commissioned

by any of the former or by the Bank may be located abroad and that data may be processed globally, including outside of Europe. During the process of registration, when making changes in relation to the Card or the Electronic Storage, and when making Mobile Wallet transactions, Client Data and Device Data as well as Mobile Wallet Operator Data is generally transmitted either in encrypted format and/or via a secure channel and where necessary across borders or globally. However, communications from the Bank for the purpose of additional authentication of the User and to confirm successful registration are transmitted in unencrypted format via an open network that is accessible to everyone (e.g. internet, SMS).

The Bank is entitled to communicate with or contact the User by SMS, email, post, pop-up in the Mobile Wallet, or other means of communication in relation to the registration process or for the purpose of notifying the User of changes to these terms and conditions for use.

Users acknowledge that third parties may be able to infer an existing contractual or other legal relationship with the Bank on the basis of unencrypted communications transmitted via an open network and that as such it cannot be assumed that the communication will remain confidential and that by extension bank client confidentiality will be retained. Users acknowledge the following risks in particular: When using a network (e.g. the internet) viruses and similar can infect the device when the device establishes contact with the network. The use of commercially available security software packages can help Users with their security precautions and is therefore recommended. There is a risk that a third party could gain access to your device unnoticed while it is being used online. Furthermore, insufficient system knowledge and a lack of security precautions for the device can facilitate unauthorized access. Network operators (e.g. internet providers) are able to trace who Users contact and when. It is important to use only software from trusted sources.

Even if the sender and the recipient are in the same country, data transmission via such networks often takes place via third countries, i.e. also via countries that do not offer the same level of data protection as the country of domicile or the location of the User. Data could be lost during transmission or intercepted, manipulated, and misused by unauthorized third parties, or the identity of the sender could be cloned or manipulated. The Bank accepts no liability for damages arising as a result.
Even with state-of-the-art security precautions, it is not possible for absolute security to be guaranteed on either the Bank or the User side. The User's device is part of the system, but it is outside the Bank's control and may become a weak link in that system. Despite all of its security measures, the Bank is unable to accept any responsibility for the device as this is not possible from a technical perspective.