Special Terms and Conditions for the participation in the 3D Secure Service

PayLife

Preamble

The Special Terms and Conditions at hand applicable to the participation in the 3D Secure Service ("STC" for short in the following) shall supplement the General Terms and Conditions (GTC) applicable to rechargeable PayLife prepaid cards ("card" for short) underlying the card contract concluded between easybank AG ("bank" for short) and the cardholder. Reference is made to the information pursuant to Zahlungsdienstegesetz (ZaDiG), the Austrian Payment Services Act, as well as pursuant to Fern-Finanzdienstleistungs-Gesetz (FernFinG), the Austrian Distance Financial Services Act, that the cardholder received before conclusion of the card contract.

The precontractual information can be found on the www.paylife.at/agb website. Moreover, it shall supplement the "Special Terms and Conditions for the Info Text Message Service", as amended from time to time.

The STC shall govern the registration for and implementation of payment transactions in secure systems. Registration for the secure systems is either started online in advance on the www.paylife.at/3dsecure website or carried out during the payment process on the Internet.

1. Definitions

1.1. Mastercard SecureCode
The password chosen by the cardholder himself/herself in the course of the 3D Secure registration process.

1.2. Mobile Transaction Number ("mobileTAN" for short)
The mobileTAN is a one-time-valid transaction number transferred to a mobile data terminal device (e.g. mobile phone, tablet) and serves as an additional identifier for card payments made with the Mastercard SecureCode. Also when registering for the 3D Secure Service and performing certain data changes in the 3D data update section, entry of a mobileTAN is required. On the www.paylife.at website, the bank provides further information on the Online Services under menu item "Service".

1.3. One-time password
The one-time password is a randomly assigned identifier serving the purpose of cardholder verification during registration for the 3D Secure Service. In the course of the 3D Secure registration process, the one-time password is replaced by entry of a self-selected password solely known to the cardholder (Mastercard SecureCode).

1.4. Secure Systems

1.4.1. 3D Secure
The 3D Secure Service is a secure system used for online payments that unequivocally identifies the cardholder as the legitimate cardholder.

1.4.2. The „https" (Hypertext Transfer Protocol Secure) Connection Protocol
This protocol serves the purpose of encrypting cardholder data and his/her personalized security details for the purpose of data transfer and thus protecting it against being spied out and misused by third parties.

2. Registration for the 3D Secure Service

2.1. Registration
Using the 3D Secure Service requires the cardholder's registration for 3D Secure. Such registration can either be started on the www.paylife.at/3dsecure website or carried out during an online payment process at a merchant (contracting company) taking part in the 3D Secure Service.

On the www.paylife.at/3dsecure website, the registration process is explained to the cardholder. For identifying the cardholder in the course of registration for the 3D Secure Service, a valid one-time password as well as a mobileTAN are required.

The mobileTAN is communicated to the cardholder via text message to the mobile phone number last specified by him/her. The bank reserves the right to offer additional channels for communicating the mobileTAN that are announced on the www.paylife.at/3dsecure website.

The one-time password is delivered in the form chosen by the cardholder himself/herself during the registration process (e.g. via e-mail or text message).

2.2. In the course of registration for 3D Secure, the cardholder is provided with the STC at hand. For the further registration process, the cardholder is required to accept the STC at hand in the place designated for this purpose whereby an agreement on the participation in secure systems ("Agreement" for short) is constituted.

2.3. The following personal identification details shall be defined by the cardholder himself/herself in the course of registration:

- User name
- Password (Mastercard SecureCode)
- Personal message (displayed during each password query for control purposes)

The cardholder can change his/her personal identification details himself/herself at any time. If the cardholder forgets the password chosen by him/her, s/he shall have the possibility to perform renewed registration pursuant to Clause 2.1. and to choose a new password in the course of such re-registration.

Disclosure of mobile phone number and e-mail address shall be required for using the 3D Secure Service. Any costs incurred for text message receipt shall be borne by the cardholder himself/herself.

3. Payment via Secure Systems

3.1. When using the card on the Internet (e-commerce), the cardholder should carry out payment instructions in secure systems. As such are deemed the 3D Secure Service (Mastercard SecureCode) and the „https" (Hypertext Transfer Protocol Secure) connection protocol. Precondition for such shall be the merchant (contracting company) (technically) enabling these.

3.2. With the password defined by the cardholder himself/herself and a mobileTAN, the cardholder can perform payment transactions in secure systems. The data communicated via text message shall be checked for correctness by the cardholder before using the mobileTAN. Only if the data transferred via text message correspond to the requested order may the mobileTAN be used for order confirmation. If the data contained in the text message deviate from the intended order, the cardholder shall inform the bank of such matter without any delay at the +43 05 99 06-6220 telephone number and stop the payment process. If, however, the card holder completes the payment process, this may constitute contributory fault in the event of any damages incurred.

3.3. If the merchant enables payment via the 3D Secure Service, the cardholder shall be obligated to perform the transactions in the framework of the 3D Secure Service.

3.4. The payment transaction, and, in particular, the payment instruction, is performed also when using the secure system pursuant to Clause 7. of the General Terms and Conditions underlying the card application. If, however, the 3D Secure Service is used, the cardholder shall enter the password chosen by himself/herself and a mobileTAN. Upon entry of password confirmation and the mobileTAN generated for this payment process, the respective amount shall be irrevocably passed for payment.

4. Secrecy

The cardholder undertakes to keep secret the personal identification details listed under Clause 2.3. and the mobileTAN in such a way as to prevent them from being accessible by unauthorized third parties. In the event of culpable violation of these obligations, the cardholder shall be liable for any damages, with liability – in the case of slight negligence – being limited to the amount of EUR 50.

5. Blockage of Access

5.1. For security reasons, the bank shall block access to the 3D Secure Service after the password has been entered incorrectly six times. As long as blockage is active, the cardholder cannot carry out payment transactions with the 3D Secure Service. In such a case, the cardholder can apply to the bank for deactivation of blockage in writing (per e-mail) or over the phone. For this purpose, the bank provides the following contact details: e-mail: paylife24@paylife.at; phone: +43 (0)5 99 06-6220.

5.2. Should the cardholder know or suspect that third parties have obtained knowledge of his/her identification details (in particular, of the password), the bank advises to change the identification details. If the cardholder should, for whatever reason, not be able to do so, s/he shall be entitled to request blockage of his/her access from the bank at any time. In such a case, the bank shall be obliged to perform blockage immediately after receipt of the cardholder's request.

6. General Provisions and Safety Notes

6.1. Changes to STC

6.1.1. Any changes to the STC shall be communicated to the cardholder to the e-mail address/postal address last specified to the bank by himself/herself. This notification shall be in paper format, or, provided that such has been agreed beforehand with the card holder, on another permanent data carrier (e.g. e-mail). Moreover, the provisions of Clause 15. of the GTC shall apply *mutatis mutandis*.

6.2. Change of cardholder's address, e-mail address and mobile phone number
The cardholder undertakes to inform the bank, in writing or via e-mail, of any change of his/her address, e-mail address and mobile phone number. This shall not affect the provision of Clause 16. of the GTC.

6.3. Safety Notes

6.3.1. As long as access to the secure systems is blocked, the card cannot be used for payments at merchants on the Internet, if such only provide the 3D Secure Service as a secure system.

6.3.2. To avoid risks associated with knowledge of the Mastercard Secure Code, the bank advises to change such at regular intervals (e.g. each month).

6.3.3. It is recommended to secure access to the use of the mobile data terminal devices. In the event of loss or theft of the mobile data terminal device, the bank recommends contacting the mobile phone service provider for the purpose of SIM card blockage.

6.3.4. Please take note of the fact that the use of passwords on shared computers and mobile data terminal devices (e.g. in an Internet café, hotel, or at the work place) enables unauthorized third parties to spy out passwords.

6.3.5. The computer and the mobile data terminal devices should be equipped with an up-to-date malware and virus protection, updated operating software as well as a firewall. Thus, the risk of data being spied out and misused by third parties can be minimized.

6.3.6. On the www.paylife.at website, the bank provides further information on secure systems as well as safety advice under menu item "Service".

7. Contract Duration and Termination

The Agreement shall be concluded for an indefinite period of time. It shall, in any event, end upon the termination of the underlying card contract or upon the ending or discontinuation of the 3D Secure Service of which the bank shall inform the cardholder without any delay.

As of July 2016, version of May 2018