Special Terms and Conditions for 3D Secure for Online Card Transactions

The below Special Terms and Conditions govern the use of the 3D Secure for online card transactions with a payment card issued by Solarisbank AG (hereinafter: “Bank”):

1. Object, Definitions

1.1 The Bank enables the holder of a card to participate in the 3D Secure process if the card is admitted for the online usage with 3D Secure that participating e-commerce retailers may provide for.

1.2 3D Secure (Mastercard calls it „Mastercard Identity Check”, VISA calls it “VISA SECURE“) is a payment authentication standard for internet purchases with a payment card.

1.3 In order to authorize online card transactions the card holder must use certain authentication elements (cf. Clauses 4.1 and 7.1 of the Conditions for Online Banking).

1.4 Authentication elements include a mobile transaction number (hereinafter: “mobileTAN”) sent to the card holder’s mobile device by SMS (Short Message Service) by the Bank; in-app authentication where card holders are redirected to the banking application of the Bank’s cooperation partners (hereinafter: “in-app authentication”); or security questions which only the card holder can answer.

1.5 The Bank may decline an online card transaction if the e-commerce retailer does not use 3D Secure.

2. Prerequisites for use

2.1 Each holder of a valid and unblocked card automatically participates in the 3D Secure procedure. Enrollment takes place when the card is activated. A separate registration is not required.

2.2 In order to perform an authentication by 3D Secure via mobileTAN, the card holder has to provide a mobile number to the Bank via one of its cooperation partners. The number may be changed at any time.

2.3 In order to perform an authentication by 3D Secure via in-app authentication, the card holder has to have successfully bound the mobile device to the account connected to the payment card.

3. Authentication via 3D Secure

3.1 The mobileTAN transmitted by SMS will consist at least of six digits and has to be entered to authenticate the online card transaction. In terms of data synchronisation, the card holder will be shown the last digits of the mobile number provided to the Bank on the screen.

3.2 The Bank will provide the SMS for free.

3.3 For in-app authentication the card holder has to login to the banking application of the Bank’s cooperation partner, to which the card holder is directed, and confirm the online card transaction.

3.4. In order to authenticate by way of answering a security question, the card holder has to give the right answer to a question only the card holder can answer.

4. Duties of care of the card holder

4.1 The card holder will take care that no third party will access the mobile device for the execution of online transactions. The bank will not ask the cardholder to enrol or deliver registration data, neither via e-mail nor via phone.

4.2 The card holder has to take steps necessary to keep the SMS secure, e.g. by password-protected access. The Bank shall not be liable where in cases of loss, theft or passing-on of the mobile device third parties obtain unauthorised access to and make use of the content of the SMS. The same applies for authentication elements used to login to the banking application of the Bank’s cooperation partner (cf. in general Clause 7.1 of the Conditions for Online Banking).

4.3 The card holder has to verify the data transferred by SMS (see Clause 3.2). In case of incorrect data, the card holder shall cancel the transaction and inform the Bank.

5. Data Processing and Service Providers

5.1 When 3D Secure is used, the card number, transaction date and time, transaction amount, merchant information (name, ID, URL) and the IP address from which the card transaction was initiated are stored.

5.2 The Bank may commission service providers to operate 3D Secure. The Bank provides these service providers with personal data of the cardholder (e.g. credit card number) exclusively within the scope of the purpose of the contractual relationship.