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_pard issued by solarisBank AG (hereinafter: "Bank"):

1. Object, Definitions

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

1.2 3D Secure (Mastercard calls it „Mastercard Identity Check, VISA calls it "Verified by VISA") is a payment authentication standard for internet purchases by a mobile transaction number (hereinafter: "mobileTAN") sent to the card holder's mobile device by SMS (Short Message Service) by the bank.

1.3 The Bank may refuse an online card transaction if the card holder wants to carry out a transaction without the use of 3D Secure at a participation retailer.

2. Prerequisites for use

2.1 Each holder of a valid and unblocked card automatically participates in the 3D Secure procedure. Registration takes place when the card is activated. A separated registration is not required. To use 3D Secure, the card holder needs his/her mobile number recorded by the Bank.

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 its cooperation partner. The number may be changed at any time.

3. Authentication via mobileTAN

3.1 If the card holder provided a mobile number to the Bank via the Bank's cooperation partner according to item 2, the Bank will basically perform an authentication via mobileTAN sent by SMS.

3.2 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.

3.3 The Bank will provide the SMS for free. Nevertheless, the Bank points out that the receipt of SMS abroad may entails additional costs issued by the mobile service provider (Roaming).

4. Duties of Care of the card holder

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

4.2 The mobile device by which the SMS with the mobileTAN will be received may not be used for the electronic card transaction at the same time. The channels of communication have to be kept separately.

4.3 The card holder has to take the necessary steps for the security of the SMS, e.g. a password protected access. The Bank shall not be liable for any losses arising out of the loss, theft or passing on of the mobile device and as a result third parties can unauthorised access and use the SMS.

4.4 The card holder has to check the data transferred by SMS (cf. item 3.2) to conformity. In case of unconformity, the card holder shall cancel the transaction and inform the Bank.

5. Data Processing and Service Providers

5.1 When paying utilizing 3D Secure, 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 process the 3D Secure procedure. 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.

6. Sign off

The card holder may at any time sign off the use of 3D Secure by informing the Bank via the cooperation partner. After signing off, gernerally no transaction can be carried out with retailers that expect an authentication with "Mastercard Identity Check" or „Verified by VISA" .