Alpha SecureWeb Terms and Conditions of Use

The “Alpha SecureWeb” service is offered by the bank with the corporate name ALPHA BANK S.A. (whose registered offices are in Athens at 40 Stadiou St., GR-10252) trading as “Alpha Bank” (hereinafter the “Bank”) and provides the customer/user of the service (hereinafter the “User”) with additional security for the electronic transactions he/she enters into. “Electronic transactions” for the purposes of these Terms and Conditions means online purchases of products and/or services within the EU using Visa, MasterCard and Diners Club cards issued by the Bank (hereinafter the “Card”) from merchants participating in the Visa Secure, Mastercard Identity Check and Diners ProtectBuy schemes respectively (hereinafter the “Merchants”) which support the secure electronic transactions protocol 3D Secure (hereinafter “electronic transactions”).

1. Acceptance of Terms and Conditions

1.1. These Terms and Conditions govern use of the Alpha SecureWeb service (hereinafter the “Service”). By using this Service the User shall be presumed to have accepted these Terms and Conditions.

1.2. These Terms and Conditions as well as the terms of the contract for issuing the Card apply to use of the Service.

1.3. The terms of the Card contract take precedence over these Terms and Conditions where there is any conflict.

2. Registration

All existing and new Cards are registered by the Bank with the Service. Consequently, the User does not need to do anything further to register his/her Card with the Service.

3. myAlpha Code authentication methods

3.1. In order to approve electronic transactions the User must authenticate him/herself using a code sent by the Bank (hereinafter "myAlpha Code”). The myAlpha Code will be sent by the Bank each time the User enters into an electronic transaction and before that transaction is completed, and may take the form of (a) a push notification or (b) a SMS/Viber message containing a unique 6-digit one-time pass (OTP) (hereinafter a “myAlpha Code sms/viber”) which will be sent where the User cannot approve the electronic transaction with the push notification referred to in point (a) above (see paragraph 4.5. and 4.6. below). The myAlpha Code sms/viber will be used in combination with a 3-digit unique number for each Card (hereinafter the “e-com PIN”). The procedure for creating that PIN is set out directly below (paragraph 3.2). The way in which a myAlpha Code is sent and how it can be used is described in detail in term 4 below.

3.2. The conditions for User authentication via push notification (para. 3.1.a above) are that the User must install the myAlpha Mobile application on at least one device (such as a mobile phone, tablet, etc.)(hereinafter the “Device”) and activate push notifications on even one of the above Devices.

3.3.1. The e-com PIN will be generated before the User completes his/her first online transaction by entering the 3-digit code he/she wants in the relevant fields which appear on the e-transaction screen, having first entered his/her Tax ID No. After that, that code will be linked to the specific Card for which it was created and, subject to paragraph 3.3.2. and 5.2 below, will remain unchanged.

3.3.2. If the User forgets the e-com PIN, he/she must contact the Bank Customer Service team to obtain a temporary e-com PIN which must be entered in the relevant field on the online transaction screen to generate the new e-com PIN which will apply thereinafter for the purpose of finalising electronic transactions.

4. Procedure for authenticating the User and approving/rejecting the transaction using a myAlpha Code

4.1. If the above conditions are met (para. 3.2.), each time the User enters into an electronic transaction

and before that transaction is completed, the Bank will send to each Device which meets the above requirements (paragraph 3.2) a push notification which the User needs to use to approve the transaction using one of the methods referred to below (paragraph 4.3). Where there are several devices, the User may use only one of the push notifications received for each transaction.

4.2. When the User receives the push notification, having selected it by pressing the Device screen, he/she must check in detail on the screen which will appear the details of the specific transaction (such as the Merchant's particulars, the amount and date of the transaction and the User's Card number) in order to approve or reject it.

4.3. Approval of a transaction using a push notification must be done using the authentication method chosen by the User and by logging into myAlpha Mobile in one of the following ways: a) using a strictly personal 4-digit personal identification number (hereinafter "PIN"), b) using the User's fingerprint (hereinafter "Fingerprint"), or c) scanning the User's face (hereinafter "Face ID")[1]. Push notifications last for a short time after which they cease to be valid.

4.4. The transaction acceptance procedure is then completed either by entering the PIN, or scanning the fingerprint or using face ID. If the User wishes to reject the transaction, he/she must select the relevant option ("Reject") on the screen displaying the transaction.

4.5. Where the conditions in paragraph 3.2 of these Terms and Conditions are met but the User does not receive the push notification for any reason (such as problem with the system, no network), he/she may select the relevant field on the transaction screen and request that the Bank send him/her either a new push notification or alternatively a myAlpha Code sms/viber, which the User will use in combination with the e-com PIN in order to approve the electronic transaction (see para. 4.7. below).

4.6. If the conditions in paragraph 3.2 set out above are not met, before completing an electronic transaction the User will automatically receive (instead of the above push notification) a myAlpha Code sms/viber at the mobile phone number recorded in the Bank's systems (following a declaration made by the User at a Bank branch or when registering at myAlpha Web) in order to approve it in conjunction with the e-com PIN, as described below (para. 4.7).

4.7. The myAlpha Code sms/viber is valid for a limited time period indicated by the Bank during which the User must enter it in the special field which will appear on his/her mobile phone screen in order to complete the transaction. This validity period will be indicated in the message itself (i.e. in the myAlpha Code sms/viber). The transaction approval procedure is completed by entering in the fields which will appear on the online transaction screen both the myAlpha Code sms/viber and the e-com PIN which the User has created (para. 3.3.1). If the myAlpha Code sms/viber and/or e-com PIN is erroneously entered more than a specific number of times, which will be indicated on the transaction screen, it will not be possible to complete the online transaction.

4.8. The User can submit a specific number of requests to re-send the myAlpha Code. That number is indicated on the screen. If the User uses up the said number of requests, requests for a new myAlpha Code for the same transaction is precluded. If a myAlpha Code is sent again for the same transaction, the transaction must be approved using the latest myAlpha Code sent.

4.9. Both the push notification and the myAlpha Code sms/viber are automated notifications/messages, cannot be reproduced and it is not possible for the User to send a response to the Bank.

4.10. The log files on the Bank's systems constitute proof in full of every myAlpha Code sms/viber and push notification sent and delivered to the User and their content, but counterevidence may also be adduced.

5. Security

5.1. The User is aware that the myAlpha Code sms/viber, the 4-digit PIN and the e-com PIN sent to the User are strictly personal so as to protect him/her from unauthorised online transactions and cannot be reproduced, and undertakes (a) to keep them secret and confidential and (b) to safeguard the Device

[1] A condition is that the User's Device has special fingerprint scanner/face scanner technology.

from any third party access when entering into electronic transactions. Under no circumstances must the User disclose the said codes to any third party or record them (even covertly) or store them in such a way that third parties can access them. Note that the Bank will never ask the User to provide any password including the PIN, myAlpha Code sms/viber and e-com PIN.

5.2. If the User suspects that any third party has acquired access to the myAlpha Code sms/viber or the 4-digit PIN or e-com PIN or his/her account on "myAlpha Mobile" via his/her Device, he/she must promptly notify the Bank using the Customer Service Line.

5.3. Where the User ascertains that unauthorised online transactions were entered into using the myAlpha Code sms/viber, e-com PIN, PIN, fingerprint or Face ID, he/she is obliged to promptly inform the Bank at the number referred to in the paragraph above.

5.4. By accepting these Terms and Conditions the User undertakes exclusive responsibility for ensuring that he/she retains possession of the Device and for effectively safeguarding and not leaking the myAlpha Code sms/viber or e-com PIN or PIN and consequently is exclusively responsible for using those codes. Where the above codes are leaked or his/her fingerprint or face ID is used without his/her consent, the User shall be obliged to take the steps outlined in paragraph 5.2 above.

5.5. In any of the cases referred to in paragraphs 5.1-5.4, the Bank shall suspend the User's ability to enter into electronic transactions. Until the Bank is notified in accordance with the above, the User shall be liable for all electronic transactions entered into and the value thereof.

5.6. The User shall be obliged to take all measures necessary to protect the Device from theft or loss during such time as he/she is using the Service.

5.7.Failure to take those steps constitutes gross negligence on the User's part with the result that he/she retains full responsibility for any transactions entered into by a third party and is obliged to pay the amounts of transactions entered into without any restriction.

6. Use of information

6.1. The Bank undertakes not to disclose any personal data of the User or information relating to him/her to Merchants with which the User enters into electronic transactions.

6.2. The Bank shall be entitled to store any email sent to or received from the User on its system for such time as is required to defend the rights and interests of both the Bank and User.

7. Suspension/termination of use of the Service

7.1. The Bank reserves the right to suspend or terminate use of the Service, other than in the cases cited in paragraph 5 above, and in the case where the User breaches any obligation deriving from the Service and any term of the contract to issue the Card.

7.2. Where ability to use the Service is terminated, the Bank shall send the User prior written notice unless for reasons of transaction security and/or User protection immediate termination of access is required, in which case the User shall be promptly notified by the Bank at the latest contact details provided to it (postal address, email address, contact phone numbers).

8. Bank obligations, liability and rights - User representations

8.1. The Bank shall be obliged to take all reasonable measures from a business perspective and to oversee the operation of the Service in order to protect the trading system software from viruses. However, the Bank shall bear no liability if despite it exercising due diligence the User's systems or files are infected with a virus.

8.2. The User acknowledges and accepts that the Bank shall bear no liability for delay, late or improper or unsuccessful receipt of messages and push notifications due to reasons attributed to or related to the provision of the User's telecom services or other factors which are not within the Bank's control (including but not limited to cases of (a) non-coverage by the mobile telephony network in a specific area, (b) exceedance of the capacity of incoming messages on the User's device, (c) maintenance of the telecommunications network, (d) malfunction of the mobile phone or incompatibility with the Service, etc.). The Bank shall not be liable for any loss incurred by the User on these grounds unless due to gross negligence or fraud on its part.

8.3. Under no circumstances does the Service guarantee nor in any manner certify the quality of goods or services which the User purchases. The choice of the counterparty the User does business with and the choice of goods or services lie exclusively at the User's discretion so that the latter assumes all relevant liability.
8.4. The Bank may, at its discretion and in accordance with the national and European legislative and regulatory framework in force from time to time, prevent certain electronic transactions from being entered into using the Service.

9. Amendment of Terms and Conditions

9.1. The Bank reserves the right to amend these Terms and Conditions and to notify them to the User either by sending a letter to that effect to the last declared postal or email address or by posting the new terms on its website. 9.2. Amendments which seek to improve or upgrade the Service provided or amendments which are imposed by law shall apply effective immediately.

9.3. Amendments which entail the User being burdened in any manner shall generate legal effects 30 days after the above notification in accordance with paragraph 9.1.

10. Personal Data

The User's digital fingerprint and biometric data collected via Touch ID/Fingerprint Scanner/Face Scanner which are installed on the Device shall be stored exclusively on the Device and shall not be sent in any manner to the Bank or to another operator/provider/administrator of the myAlpha Mobile application on its behalf, so there is no issue of any form of processing thereof by the Bank.

The notice relating to all other manners of processing of the User's personal data by the Bank has been distributed and is posted on the Bank's website at all times. (https://www.alpha.gr/el/idiotes/gdpr)