Terms of Use of the "Alpha SecureCode" Service

"Alpha SecureCode" service is offered by ALPHA BANK CYPRUS LTD (Registration No. 923), of Chilonos and Gladstonos Corner, Stylianou Lena Square, 1101 Nicosia (hereinafter the "**Bank**"), in order to provide the client - user of the "Alpha SecureCode" service (hereinafter the "**User**") with additional security in his or her electronic transactions.

For the purposes of these terms, **electronic transactions** mean the following transactions:

- Online purchases using debit or credit cards issued by the Bank (hereinafter the "**Card**") from businesses participating in the Visa Secure and Mastercard Identity Check programmes respectively, which support the 3D Secure enhanced security protocol for electronic transactions
- Money transfers to third party accounts (individuals or companies) held with the Bank via the Alpha Express Banking service
- Money transfers to other domestic or foreign banks via the Alpha Express Banking service
- Standing orders for fixed amount transfers at regular intervals to third party accounts held with the Bank
- Payments via the Alpha Express Banking service of amounts due by third parties in relation to cards and consumer loans granted by the Bank or by another domestic bank
- Payments to organisations via the Alpha Express Banking service

1. Acceptance of terms

1.1. These terms govern the use of the "Alpha SecureCode" service (hereinafter the "**Service**"). Use of the Service by the User implies acceptance of these terms.

1.2. The Service is provided under these terms, as well as under the terms and conditions of use of the Card and the terms governing the use of the Alpha Express Banking service.

1.3. In case of conflict between these terms and the terms and conditions governing the use of Alpha Express Banking and/or the Card, these terms shall prevail.

2. Registration

In order to gain access to the Alpha SecureCode service, the User must visit his or her Service Branch to register as subscriber to Alpha Express Banking.

3. Authentication methods via Alpha SecureCode

3.1. In order to authorise his or her electronic transactions, the User must be authenticated via the Alpha SecureCode service. Each time the User carries out an electronic transaction, he or she shall receive, prior to its completion:

a) a push notification (hereinafter the "push notification"); or

b) a message (SMS/Viber) containing a unique six-digit code number (OTP) (hereinafter "**Alpha SecureCode sms/Viber message**") which shall be sent in case the User is unable to authorise the electronic transaction with the push notification under point a) above, (see para. 4.5 and 4.6 below). The Alpha SecureCode sms/Viber message shall be used in combination with a four-digit unique number for each Card (hereinafter the "**ePIN**"), generated according to the procedure described below (para. 3.2). The dispatch and use of the Alpha SecureCode are described in detail in paragraph 4 below.

Note: With the combination of the Alpha SecureCode sms/Viber message and ePIN code numbers, the User can be authenticated only for online purchases using his or her Card. For the authentication of other online transactions carried out via Alpha Express Banking, push notifications must be activated.

3.2. The authentication of the User via push notifications (para. 3.1.a above) is subject to the installation by the User, on at least one of his or her devices (e.g. mobile phone, tablet, etc., hereinafter the "**Device**"), of the upgraded version of the "ALPHA BANK CY" application and the activation of the push notifications function.

3.3.1. The ePIN of the Card shall be generated prior to the completion of the User's first online purchase with his or her Card, by entering in the relevant fields displayed on the screen of the online transaction the four-digit code of his or her choice, after he or she has entered the Alpha SecureCode sms/Viber message and the Alpha SecurePIN number of his or her Card. Henceforth, this code shall be linked to the specific Card for which it was generated and shall remain the same, subject to the provisions of para. 3.3.2. and 5.2. below.

3.3.2. In case the User forgets his or her card's ePIN number, he or she should contact the Bank's Customer Service by calling the telephone number +357 22877477, in order to be given a temporary code, which he or she must enter in the relevant field of the electronic transaction screen, to re-generate the ePIN number, which shall henceforth be valid for the completion of the User's electronic transactions.

4. User authentication process and approval/rejection of transaction via Alpha SecureCode

4.1. Provided the above conditions (para. 3.2.) are satisfied, each time the User carries out an electronic transaction and prior to its completion, the Bank shall send to each Device that satisfies the above conditions (para. 3.2.), a push notification requesting the User to approve the transaction using one of the methods described below (para. 4.3.). In case of multiple Devices, the User may use only one of the push notifications received per transaction.

4.2 When the User receives the push notification, he or she should select it by tapping on the screen of the Device and thereafter verify on the screen that shall appear the details of the specific transaction, in order to approve or reject it.

4.3. The approval of the transaction via a push notification must be done by the method selected by the User for authentication and login to the 'ALPHA BANK CY' application, i.e. by one of the following: a) a strictly personal identification number (hereinafter "**PIN**"), b) his or her fingerprint (hereinafter "**Fingerprint**") or c) by face identification (hereinafter "**Face ID**")[1] . The push notification shall be valid for a limited period of time, after which it shall expire.

4.4. The transaction acceptance process is thereafter completed either by entering the PIN or by scanning the Fingerprint or Face ID. If the User wishes to reject the transaction, he or she must select the relevant field ("Reject") on the screen displaying the transaction.

4.5. In the case of online purchases using a Card whereby, even though the conditions of para. 3.2. of these terms are satisfied, the User does not receive the push notification for any reason whatsoever (e.g. system malfunction, no network coverage), he or she may, by selecting the relevant field on the transaction screen, request the Bank to send him or her either a push notification or alternatively an Alpha SecureCode sms/Viber message, which the User shall use in combination with the ePIN code number to approve his or her electronic transaction (see para. 4.7. below).

4.6. In the case of online purchases using a Card whereby the conditions of para. 3.2. above are not satisfied, the User shall automatically receive (instead of the abovementioned push notification), before completing an

[1] To enable authentication via Fingerprint or Face ID, the User's Device must be equipped with special fingerprint scanner/face scanner technology.

online purchase, an Alpha SecureCode sms/Viber message to the mobile phone number provided when registering at Alpha SecureCode in order to approve it, always in combination with the ePIN, as described below (para. 4.7.).

4.7. The Alpha SecureCode sms/Viber message is valid for a limited period of time during which the User must enter it in the special field appearing on the screen of his or her Device in order to complete the transaction. The transaction approval process is completed by entering in the fields appearing on the electronic transaction screen both the Alpha SecureCode sms/Viber message and the ePIN generated by the User (para. 3.3.1.). If the Alpha SecureCode sms/Viber message and/or the ePIN are entered incorrectly more than a certain number of times, which shall be specified on the transaction screen, it shall not be possible to complete the electronic transaction.

4.8. The User may submit a specified number of requests for resending an Alpha SecureCode sms/Viber message, as displayed on the screen. Once the User has used the aforementioned number of requests, he or she shall no longer be able to request a new Alpha SecureCode sms/Viber message for the same transaction. In case an Alpha SecureCode sms/Viber message is resent for the same transaction, the transaction shall be approved with the latest Alpha SecureCode sms/Viber message sent.

4.9. Both push notifications and Alpha SecureCode sms/Viber messages are automated notifications/messages. They cannot be reproduced and it is not possible for the User to send a reply to the Bank.

4.10. The log files recorded in the Bank's systems constitute full proof for all Alpha SecureCode sms/Viber messages and push notifications sent and delivered to the User, as well as for their content, subject to counter-evidence.

5. Security

5.1. Given that the Alpha SecureCode sms/Viber message as well as the ePIN code number sent to the User are strictly personal, in order to protect the latter from unauthorised electronic transactions, and cannot be regenerated, the User undertakes to keep them secret and confidential and to protect his or her Device from access by third parties when carrying out electronic transactions. The User must under no circumstances disclose the above codes to any third party or record them - even covertly - or save them in such manner that they can be accessed by third parties. It is noted that the Bank shall never ask the User to disclose any code number, including the ePIN and the Alpha SecureCode sms/Viber message.

5.2. If the User suspects that a third party has gained access to the Alpha SecureCode sms/Viber message and/or the ePIN code, and/or to his or her account in the ALPHA BANK CY application through his or her Device, he or she must immediately notify the Bank by contacting Customer Service at +357 22877477 or +357 22888610.

5.3. If the User finds out that unauthorised electronic transactions were made using the Alpha SecureCode service, he or she must immediately notify the Bank by contacting Customer Service at +35722877477 or +35722888610.

5.4. By accepting these terms, the User assumes the exclusive responsibility to safeguard the possession of his or her Device, as well as to effectively save and prevent the leak of the Alpha SecureCode sms/Viber message and/or ePIN and therefore becomes solely responsible for the use of these codes. In case the aforementioned codes are leaked or his or her fingerprint or facial identification are used without his or her consent, the User must follow the action described in para. 5.2 above.

5.5. In any of the cases set out in paragraphs 5.1. to 5.4. above, the Bank shall suspend the User's option to carry out electronic transactions. Until the Bank is notified as stated above, the User shall be responsible for each electronic transaction that takes place and for its price.

5.6. The User must take all necessary measures to protect his or her Device from theft or loss throughout the period of use of the Service.

5.7. Failure to comply with the provisions of paragraphs 5.1. to 5.6. constitutes gross negligence on the part of the User, as a result of which he or she shall assume full responsibility for any transactions carried out by a third party and shall be obliged to settle the amounts of such transactions, without any limitation whatsoever.

6. Use of Information

6.1. The Bank undertakes not to disclose any personal data of the User or information concerning the User to the businesses with which the User carries out electronic transactions.

6.2. The Bank is entitled to store in its system any emails sent to or received from the User, for as long as necessary, as the case may be, to protect the rights and interests of both the Bank and the User.

7. Suspension/Termination of use of the Service

7.1. In addition to the cases laid down in paragraph 5 above, the Bank reserves the right to suspend or terminate the use of the Service also in case of breach by the User of any obligation arising from the Service and/or any condition of use of his or her Card.

7.2. In case of termination of the use of the Service, the Bank shall send to the User prior written notice, unless the immediate termination of access to the Service is necessary for reasons of security of transactions and/or protection of the User, in which case the User shall be immediately notified by the Bank at the last contact details provided (postal address, e-mail address, contact telephone numbers).

8. Obligations, liability and rights of the Bank - User's Declarations

8.1. The Bank shall have the obligation to take every reasonable - in terms of trading practice - measure and to oversee the operation of the Service in order to protect the software transaction system from viruses. However, the Bank shall not be liable if, despite the exercise of due diligence on its part, the User's systems or files are infected with a virus.

8.2. The User acknowledges and accepts that the Bank shall not be liable for the delay, non-timely or inappropriate or unsuccessful receipt of messages and push notifications, for reasons attributable or related to the provision of the User's telecommunication services or other factors beyond the Bank's control (indicatively, and not limited to, cases of a) non-coverage of the mobile telephony network in a certain area, b) exceeded capacity of incoming messages on the User's device, c) maintenance of the telecommunication network, d) malfunction of the mobile phone or incompatibility with the Service, etc.). The Bank shall not be liable for any damage incurred by the User due to the above causes, unless such damage is attributed to its own gross negligence or fraud.

8.3. The Bank does not in any case guarantee or in any way certify the quality of the goods or services purchased by the User through any electronic transaction. The choice of the company from which purchases will be made and of the goods or services to be purchased shall be entirely at the discretion of the User, who shall assume all liability in this regard.

8.4. The Bank may, at its discretion and in accordance with the applicable national and European regulatory framework, exclude certain electronic transactions from the Service.

9. Amendment of Terms

9.1. The Bank reserves the right to amend these terms and to notify the User accordingly either by sending a letter to his or her last stated postal or e-mail address, or by posting the new terms on its website and/or by sending a relevant message to the Alpha Express Banking service.

9.2. Amendments aiming to improve or upgrade the Service provided or amendments imposed by law shall take immediate effect.

9.3. Amendments entailing, in any way, a charge for the User shall produce legal effects thirty (30) days after the User being notified by the Bank as per paragraph 9.1. above.

10. Personal Data

Storage of the digital fingerprint and biometric data of the User's face, as collected via Touch ID/Fingerprint Scanner/Face Scanner respectively installed on the User's Device, are stored exclusively on the said Device and are not, in any way, transmitted to the Bank or to any other entity/provider/administrator of the ALPHA BANK CY application on its behalf, so that there is no question of such data being processed by the Bank in any way. Concerning the processing of the User's personal data by the Bank in all other respects, the provisions stated explicitly in the Bank's Privacy Statement, which is posted on the Bank's website at all times, shall apply (https://www.alphabank.com.cy/AlphaBankCY/media/Media/PDFS/%ce%91%ce%925371G.pdf)