Digital wallet “my Alpha wallet”
Terms and Conditions of Use

1. Definitions

For the purposes of this Agreement the following words and expressions shall have the meanings as set out below:

“Eligible Card” means a credit, debit, or prepaid card, both personal and business (Visa, MasterCard, American Express, Diners and Maestro), which is valid, open, issued by either Alpha Bank or any other credit and financial institution, domestic or foreign, which supports the Cardholder's verification protocol of “3D Secure” type (indicatively MasterCard SecureCode, Verified by Visa, American Express SafeKey for the Card Schemes Mastercard, Visa and American Express respectively), and can be be registered to “my Alpha wallet”.

“Bank” means Alpha Bank S.A., a company with registered offices in Athens (40, Stadiou Street, 102 52) with tax registration nr. 094014249, FAEE Athinon, dully represented.

“Cardholder” means the Cardholder of Eligible Cards who has accepted these terms.

“my Alpha wallet” or “Wallet” means a digital wallet provided by Alpha Bank, in which all Eligible Cards of the Cardholder are registered, by means of which the Cardholder is able to securely conduct e-transactions. The service is more particularly described at www.myalphawallet.gr.

“my Alpha wallet mobile app” or “app”: the mobile phone application through which the Cardholder may subscribe and make use of the Wallet.

“Alpha e-Banking”: The service through which the Bank enables the Cardholder to conduct transactions and receive remote services via the Internet.

“bleep”: the mobile phone application which allows the user to proceed to the issuance of a prepaid card through a digital only procedure.

“CDI”: The personalised code number which the Bank has systemically created for each Cardholder, pursuant to which it manages him/her on a unified customer-centric basis and which proves, indicatively, amongst others, his/her identity, transactional profile and his/her contact information.

“Cardholder Identification in the Wallet with the use of fingerprint”: the identification of the Cardholder in the app with the use of the function that is supported by devices with a fingerprint censor, through which the Cardholder is identified for his/her login in the Wallet, instead of providing his/her Personal Identification Credentials.

“MasterPass Platform” means the functionality and the systems provided by MasterCard Incorporated, which facilitate payments to e-merchants’ websites bearing the mark “Buy with MasterPass”.

“MasterPass Transactions” means the payments’ transactions to e-merchants’ websites conducted through my Alpha wallet.

“Standard Checkout” process of conducting transactions means the Cardholder’s option to conclude payments to e-merchants, by connecting to his/her Wallet, after being identified in the latter by typing his/her username and secret password and after the individual confirmation of his/her payment data.

“Connect Checkout” process of conducting transactions means the Cardholder’s option to conclude payments to e-merchants, by connecting to his/her Wallet after being identified in the latter, by typing his/her username and his/her secret password, without the individual choice and confirmation of his/her payment data. Prerequisite for the use of such functionality is the Cardholder's prior consent, allowing the Wallet connection with each e-merchant, who bears the mark “MasterPass Connect Checkout”.

“Express Checkout” process of conducting transactions means the Cardholder’s option to conclude his/her transactions to specifically approved and authorized by MasterCard e-merchants, with an even faster way,
which requires neither the Cardholder’s identification by connecting to his Wallet, nor any individual confirmation of his/her payment data. Prerequisite for the use of such functionality is the Cardholder’s prior consent, allowing the Wallet connection with each e-merchant, who bears the mark “MasterPass Express Checkout”.

“Contactless Transaction” means the transaction conducted through the Tap ‘n Pay Service of the Wallet with the use of the Cardholder’s mobile phone and the mobile Application “my Alpha wallet mobile app”. The transaction is completed without the removal of the mobile phone device from the Cardholder, which must be held at a small distance from the special censor of the card acceptance device, until the system identifies it, records it and approves the transaction.

“Terms” means the terms and conditions under which my Alpha wallet shall be used.

2. **my Alpha wallet**

2.1. The Cardholder may use the Wallet:

   a) to store his/her cards’ details and other relevant information, such as the billing address for all his/her Eligible Cards,

   b) to make transactions for the purchase of goods or services provided by organizations, public services and businesses, which are associated with the Bank,

   c) as a method of payment of bills to legal entities of the public and private sector,

   d) as a method of payment to e-merchants, who accept payments through the MasterPass platform, provided by MasterCard International Incorporated,

   e) to have access to the Reward Schemes of his/her Alpha Bank card/s, being able to collect, transfer and redeem points to selected offers provided by the cooperating businesses registered to my Alpha wallet,

   f) to have access to the Bank’s “Alpha e-statements” and “Alpha alerts” services,

   g) to check the balance of each of his Alpha Bank cards, the available credit for spending, all card transactions (including the ability to print copies of them), the payment due date etc, as particularly described in the aforementioned website of the Wallet.

   h) as a method of managing his/her Alpha Bank card/s, providing the Cardholder with the following options: Card activation and any other services provided that they can be in force.

It is noted that the facilities under 2.1. (e), (f), (g) and (h) above are available exclusively for cards issued by the Bank which are registered to the Wallet, the use of which are subject to the terms of each product, as each is in force.

2.2. Aiming to the effective and appropriate use of the facilities under par. 2.1., the Cardholder acknowledges and accepts that he/she should strictly follow the detailed instructions and the informational messages that appear at every step during the use of Wallet. The Bank cannot be held liable for any administrative act or transaction conducted through my Alpha Wallet by the Cardholder, remaining the latter solely responsible for its consequences.

2.3. The Cardholder acknowledges and agrees that he/she is solely responsible for the completeness and accuracy of the information which he/she stores in his/her Wallet. The Bank cannot be held liable and/or is unable either to check or update any information stored in the Wallet or access and save the Eligible Cards’ data for its own purposes.

2.4. my Alpha wallet provides the Cardholder with the option to make electronic transactions to businesses and organizations (2.1 b & c), associated with the Bank. However, the Bank cannot be held liable for the content, the type and the value of agreements and transactions between the Cardholder and such businesses and organizations, conducted through my Alpha wallet.
2.5. If the Cardholder requires a refund due to the cancellation of any transaction conducted through my Alpha wallet, he/she shall exclusively contact the business, in which the transaction was conducted. Exceptionally, in case a transaction dispute arises, the Cardholder, apart from contacting the respective business, should also contact the Bank, or the respective credit or financial institution that issued the card, notifying the reasons for dispute, the transaction details, the applicable business address as well as any other information requested per case.

3. Registration and Account Security

3.1. In order to use the Wallet, the Cardholder is required to register for it through a strong customer authentication procedure, by providing his/her e-mail address (which will be his username), creating a secret password of his/her choice and replying to a number of security questions.

3.2. In addition, the Cardholder is required to type two random digits of his/her card's PIN, followed by a one-time password that has been sent by SMS to the Cardholder's registered mobile phone number, in order to complete the identification and registration to the Wallet of any Card issued by the Bank. The identification and furthermore the registration to the Wallet of cards issued by other credit and financial institutions, shall take place through the verification protocol “3D Secure”, provided that such protocol is used by the issuing institution.

3.3. The username and password individualize the Cardholder, serving as his/her Personal Identification Credentials with the wallet, are equal and have the same equitable effects as that of his/her Personal Identification Number (PIN) and his/her personal signature.

3.4. Upon the completion of the registration, the Cardholder, in order to activate my Alpha wallet, will receive an activation e-mail with a verification link which will be valid for 24 hours. For the Cardholder's and his/hers transactions’ safety, in case that the link expires, the Cardholder can receive a new e-mail with a verification link after following the described process at www.myalphawallet.gr.

3.5. Upon the completion of the Cardholder's registration to the Wallet by using any Card issued by the Bank, and after his/her first login to it, all cards issued by the Bank will automatically appear giving the Cardholder the option to choose if all or some of them will be registered to the Wallet. In the case that the Cardholder's registration to the Wallet has been completed with a card issued by any other credit or financial institution, all the cards issued by the Bank shall appear only if any Alpha Bank card is added to the Wallet. In any case, the Cardholder may add or remove any Card from his/her Wallet at any point.

3.6. The Cardholder agrees to provide the wallet with true, accurate, current and complete information about himself/herself, throughout the registration process. In case that any changes to the provided information occur, he/she agrees to update them in his/her Wallet, by logging into it.

3.7. The Bank may use the Cardholder’s personal information to authenticate his/her identification, while he/she is using the Wallet.

3.8. The Bank has taken all the necessary technical and organizational measures for the safety of the transactions and the collected, processed and maintained personal information and data, in order to prevent deformation, destruction or non-authorized processing and access to it, based on international standards of security and taking into account the nature of the information, as well as the hazards to which it could be exposed. The Bank reserves the right to disclose information held into its file/databases to cooperating or associated businesses in the context of support, furtherance and implementation of the electronic payments, according the provisions of existing EU and national legislation with regards to the processing of personal data, as in force.

3.9. The Bank reserves the right, according to the current compliance framework, to disclose the filed in the Wallet data to any, public or independent, organ, body or authority, which is responsible for carrying out investigation of the conduct of illegal activities, the fight against fraud, the prevention and suppression of money laundering and terrorist financing etc.

3.10. The Cardholder acknowledges and agrees that:
a) The Bank bears no liability from his/her failure to maintain accurate registration information or his/her omission to receive important information and updates about my Alpha wallet.

b) The Cardholder is responsible for protecting the confidentiality of his/her username and password, being obliged not to inform any third person about it, write or secure it wherever anyone could have access and especially to his/her mobile phone, laptop, tablet or to any other device through which he makes use of his/her Wallet.

c) The Cardholder must not give the permission to any third party to access or use his/her Wallet.

d) The Bank cannot be held liable for any losses the Cardholder may suffer, as a result of unauthorized use or misuse of his/her Wallet and the MasterPass Platform provided by MasterCard International Incorporated.

e) The Cardholder shall remain constantly informed of the security information and the recommendations provided in the Bank’s website, shall abide to them with diligence, acknowledging at the same time that the poor or incomplete implementation and compliance of the recommended security guidance, may lead to the infringement of the privacy of his/her personal data, as well as to the conduct of transactions by third or non-authorized by him/her parties.

f) The Cardholder shall inform the Bank immediately in case of any modification of his/her e-mail address and any other personal data he/she has registered. The Bank bears no responsibility for any damage the Customer may suffer due to his/her non timely notification of these changes to the Bank.

g) The Cardholder acknowledges that under the current technological capacities, the conduct of transactions through Internet is possible to bear dangers for him/her, such as, indicatively, malicious alteration or interception of the content and data transferred through Internet and declares that he/she accepts and undertakes this danger, as an inherent characteristic of these transactions.

3.11. The Cardholder must contact the Bank’s Customer Service immediately at the telephone number (+30) 210 32 60000, in any case of:

   a) any unauthorized use of his/her wallet or his/her username and password,

   b) any suspicion of any fraudulent activity or any data disclosure related to the Bank’s cards that are registered in the Wallet or the Wallet itself, or

   c) any other actual or potential security breach relating to his/her Wallet.

   Contact with the Customer Service may be recorded for security reasons.

Respectively, if the suspicion of fraudulent activity or data disclosure relates to registered cards issued by other credit or financial institutions, the Cardholder shall contact the respective issuing institution.

3.12. If any of the registered in the Wallet card is lost or stolen, the Cardholder must immediately report this to the Bank or the respective issuing credit or financial institution.

4. Use of my Alpha wallet from non registered users

4.1. In order for a non-registered user to be able to make use of the Wallet, the procedure mentioned in chapter 3 is not required, but the Cardholder may visit the Wallet’s website each time he/she wishes to use it as an external user, instead of registering to it,

4.2. In that case, the Cardholder, in order to complete any transactions within the Wallet with the use of his/her card issued either by the Bank or any other credit or financial institution, shall fill in upon every visit to the Wallet the Card’s data, with which the transaction will be conducted, as such information is not stored in the Wallet after exiting its web page.

4.3. A non-registered user cannot have full access to all aforementioned options which the Wallet provides, e.g.: conducting transactions of any kind, accessing the history log, containing the visitor’s previous transactions, even if they have been conducted with the use of the same Card. In case of
transaction’s completion failure of any kind, relevant notice will appear.

5. **Eligibility for subscription to my Alpha wallet**
   The Cardholder may only register to his/her Wallet the Cards that have been issued in his name.

6. **Use of my Alpha wallet**
   6.1. The registered user of the Wallet may use it exclusively through devices that support electronic transactions, as those are listed at www.myalphawallet.gr and according to the guidelines set therein, for the appropriate software and antivirus programmes, with which such devices should be equipped. Furthermore, in order to proceed to electronic transactions, the Cardholder shall undergo prior strong customer authentication procedure, as defined by the Bank.
   6.2. For transactions and Cardholder’s security reasons, the Bank has set a) a maximum time limit for the use of the Wallet, after the lapse of which, in case the transaction is not completed, the user is automatically logged out from the Wallet and b) a maximum number of Cardholder’s unsuccessful log in attempts, after which access to the Wallet shall be temporarily blocked and re-activated by the Cardholder, through a secure procedure for the repossession of the Cardholder’s password, as described on the Wallet’s website.
   6.3. The Cardholder accepts that by using the Wallet, he/she will conclude transactions through the internet by the use of cards registered therein, and the amount of such transactions shall in no case exceed the limits set by the Bank or the issuing credit or financial institution for each of the cards. Furthermore, the Cardholder declares that, while using my Alpha wallet, he/she will not:
   a) use the Wallet in any way that may lead to the encouragement, procurement or conduct of any criminal or other illegal activity.
   b) use the Wallet for any other purpose than the Cardholder’s own personal use.
   c) access or attempt to access the accounts of other cardholders or penetrate or attempt to penetrate any of the security measures that the Bank has applied or
   d) breach any of these terms.

7. **Login to the Wallet by the users of the Alpha e-Banking service or the application “bleep”:**
   7.1. Each Cardholder, who is also a user of the Alpha e-Banking service or the bleep app will get access to his/her Wallet, by typing his/her username and password that he/she uses to log into the abovementioned service or application.
   7.2. After his/her login by the abovementioned manner, the Cardholder will have access via the Wallet to his/her personal data as registered and shown in his/her CDI as well as to all the facilities under par. 2.1. of these Terms and Conditions.
   7.3. In case the Cardholder’s data as shown in the Wallet does not coincide with that registered in his/her CDI by the Bank as updated by the Cardholder in any way, it will be considered as valid and will appear in the Wallet as registered in his/her CDI.
   7.4. The Bank is obliged to inform in writing the Cardholders-users of the Alpha Web Banking service or the bleep app respectively in writing via all available channels that:
   i) Their log in method has changed and will now be performed as specified in par. 7.1. of these Terms and Conditions,
   ii) The abovementioned log in method constitutes henceforth their sole way of obtaining access to the Wallet and annuls access thereto pursuant to the provisions of par.3.1 of these Terms and Conditions, and
iii) In case the data of the Cardholder’s CDI does not coincide with those in the Wallet, those that is registered to his/her CDI will be considered as valid and will appear in the Wallet as his/her data (par. 7.3. above).

8. **Use of the wallet through the mobile application “my Alpha wallet app” with the additional function of identitying the Cardholder through his/her fingerprint:**

8.1. In addition to the issues defined above (par. 3.1.1.), the Cardholder may subscribe and use the Wallet through his/her mobile phone, provided that he/she downloads and installs in his/her device the “my Alpha wallet mobile app”.

8.2. With the completion of the installation of the app in the Cardholder’s mobile phone, the identification or “pairing” of the Wallet will be required, so that the Wallet will be hereinafter paired with the specific device, according to the instructions which appear on the device’s screen.

8.3. The subscribed user of the Wallet may pair the app with more than one device, provided that these have not already been paired with the app by any other Wallet user.

8.4. The “my Alpha wallet mobile app”, in addition to the functions described in term 3.1, also provides the Wallet user with the function of fingerprint identification. For his/her login in the Wallet, the Cardholder may, instead of entering his/her Personal Identification Credentials, place his/her fingerprint on the special for this purpose censor. The fingerprint is unique, individualizes the Cardholder and is equal and has the same equitable effects as typing his/her Personal Identification Number (PIN) and placing his/her personal signature.

8.5. Provided that the Cardholder has activated the fingerprint identification function in the “my Alpha wallet app”, he/she may log into the app either with the use of his/her fingerprint or, alternatively, with the use of his/her Personal Identification Credentials. These two identification methods for the Wallet login are provided simultaneously, and the use of either one does not abolish the use of the other.

8.6. The Cardholder may use more than one of his/her fingerprints for his/her identification in the “my Alpha wallet mobile app”, provided that these have been also stored in his/her device. According to the device’s software and its version, in the case of a new fingerprint addition in the device, the previous fingerprint that was stored for the user’s login in the app may be automatically deactivated, with the appearance of a respective message on the device’s screen. In this case, the fingerprint activation procedure needs to be conducted again for the user to log into the app.

8.7. In correspondence with the provisions for the Card’s PIN, which is strictly confidential and is produced electronically under full safety and confidentiality conditions, the Cardholder agrees that the registered fingerprints in his/her device relate exclusively to him/her and assumes any and all risk of the Card being charged in any transaction effected, through any fingerprint which has been registered in his/her mobile phone.

8.8. During the fingerprint identification activation, the Cardholder will be asked to select the time interval after which he/she will be required to log into the app with the use of his/her Personal Identification Credentials.

8.9. The user’s fingerprint is considered a personal data, is unique, cannot be registered, copied, reproduced, processed or stored in the Wallet, neither can it be transferred to the Bank or to any other third party.

8.10. Analytical information and guidelines with regards to the app functions, the devices, the software that supports it, the activation and the use of the fingerprint authentication option are provided in the website of the Wallet, www.myalphawallet.gr.

9. **Use of the Tap ‘n Pay Service through the mobile application “my Alpha wallet mobile app” for conducting contactless transactions with the use of mobile phones**

9.1. In addition to the terms mentioned above (article 8), the Cardholder may conduct contactless transactions in businesses which hold a card acceptance device bearing the mark “contactless” with the use of his/her mobile phone, through the “my Alpha Wallet mobile app” (hereinafter the “Tap ‘n Pay Service”).
9.2. The Bank operates the Tap ‘n Pay Service using the Host Card Emulation technology, which ensures the digital storage of data and cards’ transactions through encryption, pursuant to the security standards set by International Card Associations, whereby a new unique digital number is attributed to each Card, the last digits of which are depicted in the debit receipt which is issued by the card acceptance device of the business upon completion of each transaction through the above Service, pursuant to the provisions of par. 9.6 below.

9.3. The Cardholder may conduct contactless transactions through the Tap ‘n Pay Service exclusively with the use of a personal credit, debit or prepaid card (Visa, Mastercard, American Express), issued by Alpha Bank. On the contrary, he/she may not conduct contactless transactions through the abovementioned Service with the use of a credit, debit or prepaid business card.

9.4. The Tap ‘n Pay Service is supported by certain types of mobile phones (smartphones) in which the NFC (Near Field Communication) technology has been incorporated. The storage of the Card’s details, as well as the conduct of contactless transactions through the use of NFC technology is carried out safely, according to the international safety standards, set by the International Associations.

9.5. Activation of the Tap ‘n Pay Service, requires the login of the Cardholder in the “my Alpha wallet mobile app” and the connection of his/her mobile device to the internet.

9.6. After the Cardholder’s login in the Application, the Cardholder, upon selection of the activation of the Tap ‘n Pay Service, must follow the indicated steps which appear on the screen of his/her device and create a four-digit secret password of his/her choice “mobile PIN (mPIN)”, which will be used thereafter for the completion of each contactless transaction with the use of the Wallet through the Tap ‘n Pay Service.

9.7. In case of incorrect insertion of the mPIN 3 times, the Tap ‘n Pay Service will be blocked and transactions may not be conducted with the use of the mobile phone, until the Cardholder contacts the Bank’s Customer Service.

9.8. The secret password mPIN above individualizes the Cardholder and produces the same equitable legal effects as that of his/her Personal Identification Number (PIN) his/her personal handwritten signature. The obligations of the Cardholder referenced under par. 3.10 b above are also valid for and apply to the mPIN password.

9.9. Prior to the conduct of each contactless transaction through the Tap ‘n Pay Service, the Cardholder’s mobile phone device must be activated, without the login in the Wallet with his/her Personal Identification Number being necessary.

9.10. In order for the transaction to be executed, the Cardholder must hold his/her mobile device at a small distance from the special censor of the card acceptance device, (“POS Device”) of the businesses, which bear the mark “contactless” for a few seconds, without the removal of the device from his/her hands. Then, once the transaction is identified and appears on the screen of the device, the Cardholder must type the mPIN password for the completion of the approval of the transaction. Alternatively, the Cardholder may log in to the Application and after selecting the Tap ‘n Pay option, he/she shall firstly introduce the mPIN and afterwards hold his/her mobile phone at a small distance from the special sensor.

9.11. The typing of the mPIN password by the Cardholder is required for the completion of each contactless transaction, regardless of its amount and implies his/her unconditional and irrevocable acceptance and authorization for the charging of his/her Card which is stored in the Wallet with the consideration thereof.

9.12. Each contactless transaction is completed upon connection of the POS device to the Bank’s electronic systems, so that the available balance of the account may be checked in real time and the equal charge thereof approved through the respective indication on the card acceptance device (accept/deny) and the issuance of the relevant receipt from the card acceptance device (POS), equivalent to the amount of the transaction which took place, which is delivered to the Cardholder. All the transactions approved shall appear on the Card’s activities in the Wallet.

9.13. Apart from the above, the Cardholder may not conduct any other kind of transaction through the Tap ‘n Pay Service, such as cash withdrawal from ATMs or branches.
9.14. By analogy to the provisions of par. 3.10 e’ above, the Cardholder shall at all times follow and comply immediately with the instructions and suggestions which may be sent to him/her via respective messages through the Wallet. Such instructions and suggestions concern the updating of the parameters related to the Service and the security of the transactions conducted through it, including but not limited to the indicated actions for the renewal and updating of the necessary “keys”, which are required for the conduct of each contactless transaction through the connection of the mobile phone device to the internet etc.

9.15. Analytical information and instructions for the operation and use of the Service are provided in the “my Alpha Wallet mobile app”.

10. **Conducting transactions through the MasterPass Platform, provided by MasterCard International Incorporated**

10.1. In case of e-merchants bearing the mark “MasterPass”, the Cardholder, after selecting through the business’s website the product or service that he/she wishes to purchase, has the option to complete his/her payment by using the Wallet. The completion of such transaction is conducted through the above-mentioned MasterPass Platform.

10.2. The Cardholder in order to complete the transaction in the e-merchant's website shall click on the MasterPass icon, from where he/she is transferred directly to the MasterPass platform's safe link, through which he/she is connected to my Alpha wallet. Thereafter, he/she shall subsequently select and confirm the Card that he/she will use for the payment and register other identification data required for its execution.

10.3. Upon the completion of each payment transaction to any e-merchant, the Cardholder is provided with the option to select among the following procedures of payment, i.e. “Standard Checkout”, “Connect Checkout”, or “Express Checkout”, as listed in the definitions of these terms.

10.4. By choosing “Connect Checkout” or “Express Checkout” as the procedures of payment, the Cardholder accepts the transmission to the e-merchant of his/her Cards’ data, specifically protected and masked, as well as the transmission of his/her address data. The Bank shall not be held liable for the collection, use and the privacy policy that each business adopts for its clients.

10.5. In compliance with paragraph 6.2, the completion of each payment transaction to any e-merchant shall be completed within a maximum time limit from the moment that the Cardholder has logged in to his/her Wallet. If this time limit, which is set for the Cardholder’s and transactions’ security, expires without the payment process being successfully completed, the Cardholder shall be asked to repeat it. The time which the Cardholder spent in the business’ website is not included in the aforementioned time period, but only the time during which he was logged in the Wallet.

11. **Charges**

The Bank applies no charges for the provision of my Alpha wallet or the “my Alpha wallet app”. For any changes on the matter, the Wallet holder will individually be informed with the use of the contact information that he/she has stored in his/her Wallet, as well as through www.myalphawallet.gr.

12. **Use of my Alpha wallet and other wallets**

12.1. The Cardholder shall not create wallets, either jointly owned or on behalf of corporate entities.

12.2. The Cardholder is able to hold other digital wallets with other providers at the same time as holding the Wallet.

12.3. The Bank cannot guarantee that any Eligible Card will be accepted through the registration process in the Cardholder’s Wallet.

13. **Termination and Suspension**

13.1. The Cardholder may terminate his/her Wallet at any time by logging into my Alpha wallet website and removing from it all his/her cards or by contacting the Alpha Bank Customer Service on (+30) 210 32
The Bank may suspend, discontinue or terminate the Cardholder's access to the use of his/her Wallet and/or my Alpha wallet at any time, immediately and without prior notice to the Cardholder a) in case the Wallet becomes empty of any cards after the deletion of all the registered Cardholder's cards from it, b) for objective safety reasons, if he/she is suspected for conducting fraudulent transactions or/and demonstrating illegal behavior, c) upon suspicion of money laundering and terrorist financing, d) upon relevant application of the card issuer, e) in case the Cardholder misuses the MasterPass Platform, as well as, f) In any case the Cardholder breaches any of these terms, or g) Upon the Bank’s discretion, for any other reason. In case of scheduled temporary block of the Service (i.e. due to upgrade workings known beforehand), the Cardholder shall receive a notification e-mail for the inability to use the Wallet, along with relevant suggestion to contact the Bank’s Customer Service for further information and required actions, if any, for such block cessation. In case of the Service’s temporary block, due to emergency and unforeseen reasons, the Bank shall notify the Cardholder by any suitable means.

The Cardholder agrees that the Bank shall not be held liable for any suspension, discontinuance, termination, change or modification of his/her use or access to the Wallet.

Upon termination of the Cardholder’s access to my Alpha wallet, he/she remains liable for all payments made and other obligations that the Cardholder has undertaken under these terms.

If the Cardholder’s Wallet is terminated, the Bank will fulfill all of its legal obligations related to previous transactions conducted with the use of the Wallet. The Bank will keep available to the Cardholder all his/her relevant data for a period of 90 days from the date of the Wallet’s termination. The Bank will also provide any data required in case of a dispute.

14. Liability

Nothing in these terms shall exclude or limit the Bank’s liability for fraudulent misrepresentation, resulting from negligence by the Bank, its employees or its agents.

Despite of the Bank having taken all necessary security measures, the Bank cannot be held liable for any damage that may occur to the Cardholder’s computer system, device hardware or software or loss of data that results from the use of the Wallet. The Bank does not guarantee that any files that the Cardholder downloads relating to the Wallet are free from viruses, contamination or destructive features. The Bank shall not be held liable for any damage of the Cardholder’s devices, used for Wallet purposes, for any reason, including also the lack of the appropriate antivirus programme.

The Bank does not guarantee that the Wallet will be always available, uninterrupted and in full operating condition. Access to my Alpha wallet may be suspended temporarily and without any prior notice in case of system failure, maintenance or repair or for any reasons beyond the Bank’s control.

In addition to paragraph 12.2, the Bank assumes no responsibility for any losses, because of access to third party websites, that may caused to the Cardholder using his/her Wallet in order to conduct transactions. The Bank does not guarantee the uninterrupted operation of these websites, and bears no liability towards the Cardholder in case of fraudulent transactions, loss of data or any other loss may incur by using it.

The Bank does not guarantee the continuous and uninterrupted functionality of MasterPass Platform, which is supported and provided exclusively by MasterCard International Incorporated.

The Cardholder will be responsible for any reasonable losses suffered by him/her and/or the Bank, as a result of any breach of these terms by him/her.

The Bank does not accept and is not liable for the content of other websites or the websites to which they link via hyperlinks or advertising banners.

15. Changes to Terms and Conditions

The Bank may amend these terms at any time, after notifying the Client a priori, with the use of
his/her contact information that has been registered in his/her Wallet or through Alternative Networks, which he/she uses or through any other appropriate means. These changes will also be posted on the Wallet’s website.

15.2. The notification mentioned above shall be sent at least 60 days before the initiation of validity of the new terms. The client has the right not to accept the amendments and delete his Wallet immediately, without any charge until the date of initiation of validity of the amendments. The Cardholder will be deemed to have accepted any such changes by the Cardholder’s continued use of the Wallet from such time.

15.3. Amendments for improvements or upgrade of the provided hereby services shall have immediate effect.

15.4. Any use of the Wallet by the Cardholder implies the unconditional acceptance on his/her behalf of these terms as applicable

16. General Terms

16.1. The Cardholder agrees that if any provision of these Terms are deemed unlawful, void or for any reason unenforceable, that provision shall be deemed severable from these Terms and shall not affect the validity and enforceability of any remaining provisions.

16.2. The Bank may transfer or assign the Bank’s rights and obligations under these Terms to another organization and it will notify the Cardholder in writing if this happens. These Terms will then apply to them in the same way as they applied to the Bank. However, the Cardholder cannot transfer or assign his/her rights or obligations under these Terms to anyone else.

16.3. The registration of the Cardholder to my Alpha wallet and the hereafter use of it results in his/her unconditional acceptance of these Terms, which add to and specialize the “Cooperation Framework – Terms of Banking Transactions, Individuals version 1.0/2010” and the terms of credit or/and prepaid cards, with the use of which the transactions through Wallet might be concluded.

16.4. These Terms are governed by the Greek Law and any dispute arising from the above will be submitted to the jurisdiction of the Courts of Athens.
IN ADDITION TO THE TERMS AND CONDITIONS OF USE OF MY ALPHA WALLET YOU AGREED TO WITH ALPHA BANK, IF YOU DO NOT AGREE WITH THE FOLLOWING MASTERCARD INTERNATIONAL INCORPORATED ("MASTERCARD") TERMS, PLEASE DO NOT USE MASTERPASS OR THE MASTERCARD SITE. IN NO EVENT SHALL MASTERCARD OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, EXEMPLARY, CONSEQUENTIAL OR ANY OTHER DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO PROPERTY DAMAGE, LOSS OF USE, LOSS OF BUSINESS, ECONOMIC LOSS, LOSS OF DATA OR LOSS OF PROFITS, WITHOUT REGARD TO THE FORM OF ACTION (INCLUDING BUT NOT LIMITED TO CONTRACT, NEGLIGENCE, OR OTHER TORTIOUS ACTIONS) ARISING OUT OF OR IN CONNECTION WITH YOUR USE OR ACCESS TO MASTERPASS OR FROM ANY INFORMATION, CONTENT, MATERIALS, PRODUCTS (INCLUDING SOFTWARE) OR OTHER SERVICES INCLUDED IN OR OTHERWISE MADE AVAILABLE TO YOU THROUGH MASTERPASS, YOUR WALLET PROVIDER, THE MASTERCARD SITE OR ITS CONTENT, EVEN IF MASTERCARD OR ITS BUSINESS PARTNERS, EMPLOYEES, REPRESENTATIVES OR AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE OR LOSS. NOTWITHSTANDING THE FOREGOING, THE MASTERCARD PARTIES' TOTAL LIABILITY TO YOU FOR ALL DAMAGES, LOSSES, AND CAUSES OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING, BUT NOT LIMITED TO, NEGLIGENCE), OR OTHERWISE SHALL NOT, UNDER ANY CIRCUMSTANCES, EXCEED ONE HUNDRED DOLLARS ($100). THE FOREGOING LIMITATIONS AND EXCLUSIONS APPLY EXCEPT TO THE EXTENT EXPRESSLY PRECLUDED BY APPLICABLE LAW. IN SUCH JURISDICTIONS, ALL OR A PORTION OF THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU AND THE SCOPE AND DURATION OF THE MASTERCARD PARTIES' WARRANTIES AND THE EXTENT OF THEIR LIABILITY WILL BE THE MINIMUM PERMITTED UNDER SUCH APPLICABLE LAW. 

MASTERPASS IS PROVIDED “AS IS,” “AS AVAILABLE,” AND WITH ALL FAULTS. THE MASTERCARD PARTIES DISCLAIM ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY, QUALITY OF INFORMATION, QUIET ENJOYMENT, NON-INFRINGEMENT, TITLE, OR FITNESS FOR A PARTICULAR PURPOSE. MASTERCARD DOES NOT WARRANT THAT THE INFORMATION CONTAINED IN MASTERPASS, OR ON ANY THIRD PARTY SITE WILL BE ACCURATE OR COMPLETE, OR THAT MASTERPASS OR ANY THIRD PARTY SITE WILL BE ERROR FREE, UNINTERRUPTED, FREE FROM SPYWARE, MALWARE, ADWARE, VIRUSES, WORMS, OR OTHER MALICIOUS CODE, OR WILL FUNCTION TO MEET YOUR REQUIREMENTS. MASTERCARD DOES NOT WARRANT THAT MASTERPASS WILL WORK WITH YOUR OPERATING SYSTEM OR WITH ANY OTHER SOFTWARE INSTALLED ON YOUR COMPUTERS OR MOBILE DEVICES. INFORMATION OBTAINED BY YOU FROM MASTERCARD WILL NOT CREATE ANY WARRANTIES. YOU ASSUME ALL RISKS ASSOCIATED WITH YOUR USE OF MASTERPASS. IT IS YOUR SOLE RESPONSIBILITY TO DETERMINE WHETHER MASTERPASS IS SUITABLE AND ADEQUATE FOR YOUR NEEDS. YOU SPECIFICALLY ACKNOWLEDGE THAT MASTERCARD DOES NOT HAVE ANY CONTROL OVER YOUR PAYMENT INFORMATION TRANSMITTED BY MASTERPASS ON YOUR BEHALF, AND MASTERCARD CANNOT ENSURE THAT ALL TRANSACTIONS WILL BE COMPLETED OR THAT THE PARTY WHO HAS ISSUED YOUR CARD OR REWARDS NUMBER, AS APPLICABLE, WILL AUTHORIZE THE TRANSACTIONS THAT YOU INITIATE.