Safe@Web Service

Important Information and Terms and Conditions for the Use of the Safe@Web Service

PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE USING THIS SERVICE

The Cards Terms and Conditions and Prepaid Cards Terms and Conditions which apply to your Card and 1Bank Terms and Conditions, remain in full force and effect. The present Safe@Web Terms and Conditions (the "Safe@Web Terms") are a legal agreement between you and the Bank and only govern the use of the Safe@Web Service.

By using the Safe@Web service, it means that you agree to these Terms and Conditions

Safe@Web is the service offered by the Bank of Cyprus Public Company Ltd to its Cardholders, in accordance with these Safe@Web Terms. Safe@Web adds security to the online purchases made by Cardholders, by authenticating their identity at the time of a purchase via the 3D Secure technology platform. The 3D Secure technology platform has been developed by Visa and MasterCard and is called (a) Visa Secure and (b) Mastercard® Identity Check™ service, as the case may be, depending on the Card you are using. The Safe@Web service applies to online purchases made from merchants participating in the Visa Secure and/or Mastercard® Identity Check™ services.

The use of the Safe@Web service is governed by these Safe@Web Terms, which relate to your relationship with the Bank only. Please download and save or print a copy of these Terms for your records.

The Safe@Web Terms are provided in addition to the Cards Terms and Conditions, the Prepaid Cards Terms and Conditions (as the case may be, depending on the Card(s) you are using) and/or any other agreement governing the relationship between the Bank of Cyprus Public Company Ltd and the Cardholder including, without prejudice to the above, the Terms and Conditions of 1bank, if applicable.

In case of conflict between these Terms and Conditions and the Card Terms and Conditions and/or the Prepaid Cards Terms and Conditions and/or the 1Bank Terms and Conditions and/or any other agreement governing the relationship between the Bank of Cyprus Public Company Ltd and the Cardholder, these Safe@Web Terms and Conditions shall prevail with respect to the Safe@Web service. These Safe@Web Terms and Conditions as well all other terms and conditions and/or agreements as mentioned above, as amended from time to time, can be found on the website of the Bank of Cyprus Public Company Ltd www.bankofcyprus.com.

1. DEFINITIONS

1.1**.**

“1bank’’ means the 24-hour electronic service provided by the Bank in order to allow the Users of 1bank to have access to and use its Services, including the provision of information, the execution of banking transactions as well as to provide to other persons general information by any digital channel including the telephone, internet, mobile application or by other means of communication the Bank may determine from time to time.

“1bank Terms and Condition’’ means the Terms and Conditions governing the access to and use of 1bank services by any User as may be amended, extended or replaced from time to time by the Bank and notified to the User, the Company and/or to the Account Holder in accordance with paragraph 18 of the 1bank Terms and Conditions.

"Bank" means the Bank of Cyprus Public Company Ltd registered with the Registrar of Companies and Official Receiver in Cyprus (Reg.No.165), having its registered office at 51 Stassinos St., Strovolos 2002 and licensed by the Central Bank of Cyprus. The definition also includes its successors, assignees and any person acting on its or their behalf.

‘Call Centre’ means the Bank’s call centre at 800-00-800 or +357-22128000 (if calling from abroad) that offers telephone assistance to customer for various services, including Card Transactions.

"Card" means the payment instrument which may be issued in plastic or other form by the Bank to a person and confers on this person the possibility to effect the Transactions defined in the Cards Terms and Conditions or the Prepaid Cards Terms and Conditions and includes the Visa Card, MasterCard, or a Card on any other card acceptance scheme, any renewal, replacement and any additional cards including, without limitations, any contactless card in a wearable form, all of which can be debit, credit or charge cards or electronic cards.

"Card Account" or **“Account"** means an account maintained by the Bank in relation to Transactions taking place from the use of the Card(s).

"Cardholder" means the person who has requested the issue of the Card (whether to the Cardholder himself or to an Authorized Cardholder) who is given the permission to use the Card in accordance to the Cards Terms and Conditions and includes his personal representatives and heirs.

"Cards Terms and Conditions" and “Prepaid Cards Terms and Conditions’’ (respectively) means the terms and conditions governing the issuing and use of the Cards, or Prepaid cards, signed or to be signed or otherwise applicable between the Bank and a Cardholder.

"Mastercard® Identity Check™ " is the brand name by MasterCard for its service with regards to providing the 3D Secure technology platform for online purchases developed by MasterCard.

“Mobile Number” is the Cardholder’s mobile number that is registered in the Bank’s records.

"One-Time Password" or “OTP” is the security code, with temporary validity and for single use, which is sent to the Cardholder via Short Messaging Service (“SMS”) to his/her Mobile Number.

"Participating Merchant" means a merchant participating in the Visa Secure and/or the Mastercard® Identity Check™ services.

“Passcode” means the personal identification number created by the User, to be used in conjunction with the User ID of the User and, where appropriate, with the dynamic password produced by the Device /Mechanism Producing Single Use Codes or by another 1bank Payment Instrument the Bank may specify from time to time.

“Payment Services” have the same meaning given by the Provision and Use of Payment Services and Access to Payment Systems Law of 2018.

"Safe@Web" is the service offered by the Bank for using a Card under the Visa Secure and/or the Mastercard® Identity Check™ services.

"Transaction" means any transaction whereby goods or services are obtained by the use of the Card, the Card number or in any different manner by which the Cardholder or the Authorized Cardholder gives his authorization to debit the Card Account.

"Visa Secure" is the brand name by Visa for its service with regards to providing the 3D Secure technology platform for online purchases developed by Visa.

“User ID” means the number allocated by the Bank to the User for use in conjunction with the Passcode and, where applicable, with the dynamic password created by the Device/Mechanism Producing Single Use Codes or by another 1bank Payment Instrument the Bank may specify from time to time.

“you” means a customer of the Bank, and includes the primary Cardholder and each supplementary Cardholder or authorised user of a Card.

1.2 In this document, words importing the masculine include the feminine and vice versa.

2. USING THE SAFE@WEB SERVICE

2.1 All Cards issued by the BANK are automatically enrolled and participate in the Safe@Web service. It is not a requirement to register for the service prior to using the Card online.

2.2 Participating Merchants will show the Visa Secure and/or Mastercard® Identity Check™ logo.

2.3 In certain situations during the payment process on the Participating Merchant screen, the Cardholder may be required to proceed with the authentication process before the transaction is forwarded to the Bank for authorization.

2.4 Whenever authentication by the Cardholder is required, a Safe@Web screen is displayed on the Cardholder's desktop, mobile or other digital device. (a necessary condition for this authentication process is for the Cardholder to be a 1Bank subscriber).

2.4.1 Two authentication process methods are available, as follows:

A. If the Cardholder is a 1Bank subscriber and does not use the BOC Mobile App on his mobile phone and/or has not activated the 'notifications' in the BOC Mobile App, the authentication process is done as follows:

STEP 1 (Screen 1):

An OTP is generated by the Safe@Web system and sent to the Cardholder's Mobile Number. The Cardholder will be required to enter the received OTP in the designated box on the Safe@Web 1st screen.

STEP 2 (Screen2):

After the OTP has been entered, a 2nd screen follows to complete the Cardholder's authentication process, where he/she will have to enter his/her Passcode (1Bank).

Upon successful entry of the above, the Transaction is forwarded to the Bank for authorisation.

There is a limited number of consecutive attempts to enter a valid OTP and Passcode. When the OTP and/or Passcode is invalid, an error message will appear on the Safe@Web screen. After the maximum permitted failed attempts to enter a valid OTP and/or Passcode on the Safe@Web screen, the Transaction cannot be processed and is cancelled. You will therefore need to visit the Participating Merchant's website again to re-enter your Transaction.

B. If the Cardholder is a 1Bank subscriber with active 'notifications' on the BOC Mobile App, the authentication process will be as follows:

The Cardholder will receive a push notification on his/her registered trusted device. The Cardholder will be asked to verify the Transaction through the Boc Mobile App. The Transaction details will then be presented to the Cardholder on the Boc Mobile App for review. If the Cardholder's authentication process is confirmed and he/she accept the Transaction details in the Boc Mobile App, then the transaction is forwarded to the Bank for authorisation.

2.5 For a small percentage of Transactions, the authentication process will not be triggered and the Transaction may be forwarded for authorization directly or may be declined, for security and prevention purposes. Should this occur it does not necessarily mean that any subsequent authentication requests the Cardholder makes, will be declined as well. The Cardholder may contact the Call Centre as per sub-clause 3.2 for more information.

2.6. The Cardholder must follow all instructions and information regarding Safe@Web which are available at the Bank's website www.bankofcyprus.com.

2.7. The Bank reserves the right to introduce, at its absolute discretion, a fee for the use of Safe@Web in the future and to notify the Cardholder accordingly in any way it shall decide.

3. SECURITY

3.1 The Cardholder must keep all his personal data and his/her OTP and the Passcode confidential, at all times including, without limitation, by not disclosing it to anyone or writing it down or otherwise recording it in any way that may be accessible or understood or found by anyone other than himself.

3.2 If a Cardholder suspects or knows that someone other than himself may use or has used Safe@Web with his/her personal data and/or Mobile Number and/or mobile device through the Bank's mobile app and/or can obtain or has access to or knows his/her OTP and/or Passcode, he/she must immediately notify the Bank at any of the following telephone numbers: Call Centre: 800-00-800 or +357-22128000 (if calling from abroad) in order for the Bank to block the Card. During the non-working hours of the Call Centre, the Cardholder must immediately contact JCC Payment Systems Ltd at +357 22868100, to block his/her Card(s).

3.3 If the Cardholder suspects or knows that any fraudulent or unauthorized Transactions have been carried out through Safe@Web, he/she must immediately notify the Bank as mentioned above.

3.4 The Bank has the right to immediately block a Cardholder's Card in the cases provided in sub-clauses 3.2 and/or 3.3 above. The Bank shall inform the Cardholder of its decision and the reasons for it, before or immediately after the blocking of the Card, unless the provision of such information by the Bank to the Cardholder is prohibited under European or national law or such information would compromise objectively justified security reasons.

3.5 The Bank and/or JCC Payment Systems Ltd, being authorized by the Bank (or any other person which may be authorized and announced by the Bank from time to time) may contact the Cardholder by telephone, using the contact details held in the Bank's system, in cases where there is a suspicion of fraud or security threat and/or for operational reasons and/or in an effort to avoid the misuse of the Cardholder's personal data and/or Mobile Number and/or OTP and/or Passcode.

4. PERSONAL DATA AND PRIVACY STATEMENT OF THE BANK

4.1 The Bank will process the Card number, the Mobile Number of the Cardholder and the relevant Transaction details for the purposes of the Safe@Web service. This data may be provided to third parties for the purposes of making the Safe@Web service available.

4.2 These Safe@Web Terms should be read alongside the Bank's Privacy Statement, which can be found on the Bank's website at www.bankofcyprus.com.The Privacy Statement sets out more detailed information about the Bank's use of personal data. You should review the Privacy Statement to ensure that you understand how the Bank processes your personal data and you understand your rights with respect to this processing. The Privacy Statement may be amended or replaced in accordance with the terms stipulated in that document.

5. LIMITATION OF LIABILITY OF THE BANK AND DISCLAIMER

5.1 The Bank shall not be liable for any inconvenience and/or loss and/or damage and/or delay incurred by or caused to a Cardholder and/or the holder of the Card Account from the use of or inability to use the Safe@Web service due to any of the following:

i. a breach by the Cardholder of any provision of these Safe@Web Terms and/or a breach by the Cardholder and/or the holder of the Card Account of any other applicable terms and conditions of and/or agreements with the Bank;
ii. any delay and/or technical malfunction and/or failure and/or interruption of the Internet and/or the mobile telecommunication services and/or any wireless connection and/or of the website of any Participating Merchant and/or of any electronic system and/or software and/or settings and/or equipment and/or devices and/or hardware used for access and/or use by the Cardholder to Safe@Web and/or for the use by the Cardholder of Safe@Web and/or for authentication process by the Cardholder through Safe@Web, including access to the website of any Participating Merchant/s, and/or from any virus and/or malware affecting any of the above;
iii. failure of the Cardholder to enter the OTP and/or the Passcode correctly;
iv. a telephone and/or other mobile and/or communication device of the Cardholder being lost or stolen, damaged or exposed to abuse or used in an unauthorized manner without the Cardholder's consent, hacked or due to the installation of any virus and/or malware to such device.
v. where the personal data and/or Mobile Number that the Cardholder has provided and/or provides when requested by the Bank is not correct and/or updated and/or is inadequate and/or incomplete and/or is not provided at all. The Bank will not be liable for any inconvenience and/or loss and/or damage incurred or caused due to any change of such personal data and/or Mobile Number for which the Cardholder has not properly and adequately notified the Bank. The Cardholder will be able to notify the Bank by contacting the Call Center as per clause 3.2 above or

by visiting any branch of the Bank or by using any other method accepted by the Bank.

5.2 The Bank shall not be liable for any loss and/or damage resulting from any delay or omission by a Cardholder and/or holder of the Card Account to notify the Bank for any suspected or otherwise unauthorized use of his/her/their personal data or OTP and/or Passcode for access to and/or use of Safe@Web.

5.3 Subject to any applicable law, the Cardholder shall be liable for every use of the personal data and/or Mobile Number that he provided and/or his OTP and/or Passcode in relation to Safe@Web, unless it is the result of fraud or gross negligence of the Bank or any third party providing services to and/or acting as agents of the Bank and/or any subsidiary and/or affiliate company of the Bank which is involved in the provision of the Safe@Web service by the Bank to the Cardholder.

5.4. The Bank has no control over and cannot and will not warrant accessibility to or the safety of any websites of a Participating Merchant and/or any other third party, whether these are accessed by the Cardholder directly or through links on the official website or otherwise by or through the Bank. Such websites are constructed and designed at the exclusive discretion and with the exclusive liability of their owners and/or the persons maintaining them, and the Bank cannot and will not censor or edit or approve or be responsible or liable for the content or privacy policies or practices of such websites, or for the correctness, legality, completeness, appropriateness and/or accuracy of information in such websites, or for the quality or fitness or attributes of products and/or services available in such websites and/or links, whether a Cardholder purchases such products or services or not.

Furthermore, the Bank will not be responsible or liable for faults in and/or bad administration of such websites and/or for any loss and/or damage to any user or visitor including, without limitation by access to and/or use of software, information, services and/or products of such websites and/or links.

5.5. The Cardholder's correspondence or business dealings with, or participation in promotions of, Participating Merchants, including payment and delivery of related goods or services, and any other terms, conditions, warranties, or representations associated with such dealings, are solely between the Cardholder and such Participating Merchant. The Bank shall not be responsible or liable for any loss or damage of any sort incurred as the result of any such dealings. The availability or use of the Safe@Web service does not, in any way, indicate that the Bank recommends or endorses any Participating Merchant, regardless of whether the merchant participates in the Mastercard® Identity Check™ service and/or Visa Secure service. For example, the Safe@Web service does not verify the identity of the merchant or the quality of the merchant's goods or services.

5.6. The Bank shall not be liable for any disruption and/or failure to provide Safe@Web and/or any loss and/or damage to the Cardholder and/or holder of the Card Account from such disruption and/or failure, which is the result of any events outside the reasonable control of the Bank, including, without limitation, acts of God (including fire, flood, earthquake, storm, hurricane or other natural disaster), pandemics, war, invasion, acts of foreign enemies, hostilities (regardless of whether war is declared), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation, terrorist activities, nationalization, government sanction, blockage, embargo, labour dispute, strike, lockout

or interruption or failure of electricity or telephone and/or other communication services. In such an event the Bank will take all reasonable steps to restore Safe@Web the soonest (where this is reasonably possible) and to minimize delay and/or damages caused by foreseeable events.

5.7. Without limitation or prejudice to any other provision of these Safe@Web Terms, the Bank shall not be liable in the event of failure to comply with its obligations towards the Cardholder and/or the holder of the Card Account under these Safe@Web Terms, if such failure:

i. is due to abnormal or unforeseen circumstances outside the Bank's control the effects of which cannot be avoided despite the Bank's reasonable efforts to the contrary, or
ii. the non-compliance is due to the Bank's obligations under European or national law.

5.8. Under no circumstances will the Bank be liable for direct, indirect, consequential, incidental, special or indirect losses or other damages, such as loss of profit and/or any damage to the Cardholder's computer or telephone service or mobile or other communication device, resulting from the Cardholder's use of Safe@Web.

5.9. This clause 5 shall survive any termination of these Safe@Web Terms, howsoever caused.

6. BLOCKING A CARD, SUSPENSION AND TERMINATION OF THE SAFE@WEB SERVICE AND OF THESE SAFE@WEB TERMS

6.1. Without limitation or prejudice to any other rights of the Bank under these Safe@Web Terms, the Cards Terms and Conditions and/or the Prepaid Cards Terms and Conditions (as the case may be) and/or any other agreements of the Bank with the Cardholder and/or the holder of the Card Account, the Bank may block the Card immediately if the Cardholder and/or holder of the Card Account informs the Bank or if the Bank is otherwise informed or suspects that:

i. a person other than the Cardholder is attempting to use or is using or has used the Cardholder's personal data and/or his OTP and/or Passcode
ii. a person other than the Cardholder knows or can gain knowledge of the Cardholder's OTP and/or Passcode
iii. a Cardholder's OTP and/or Passcode has been and/or is being used illegally
iv. a Cardholder has breached these Safe@WebTerms and Conditions or the Card Terms and Conditions or the Prepaid Cards Terms and Conditions (as the case may be)
v. the Card Terms and Conditions or the Prepaid Cards Terms and Conditions (as the case may be) are terminated in accordance with the provisions of the Cards or Prepaid Cards Terms and Conditions and/or the Cardholder's Card has been blocked, for any reason in accordance with the Cards or Prepaid Cards Terms and Conditions.

The Bank shall inform the Cardholder of its decision and the reasons for it, before or immediately after the blocking of the Card, unless the provision of such information by the

Bank to the Cardholders is prohibited under European or national law or such information would compromise objectively justified security reasons.

6.2. The Bank will suspend and/or terminate a Cardholder's use of Safe@Web immediately if required to do so by the provisions of any applicable law.

6.3. The Bank may suspend and/or terminate the use of Safe@Web by a Cardholder if requested to do so by any third party providing services to and/or acting as agent of the Bank and/or by any subsidiary and/or affiliate company of the Bank which is involved in the provision of the Safe@Web service by the Bank to the Cardholder, provided that such request is in accordance and/or in compliance with and/or does not violate any applicable law.

6.4. The Safe@Web service and its use by the Cardholder may be suspended and/or terminated if and when the Visa Secure service and/or the Mastercard® Identity Check™ service is/are suspended and/or terminated.

6.5. Without limitation or prejudice to the abovementioned provisions, the Bank may terminate a Cardholder's use of Safe@Web without providing any reasoning by giving a two (2) months' notice in a way that the Bank considers appropriate.

6.6. The Cards Terms and Conditions and/or the Prepaid Cards Terms and Conditions (as the case may be) and/or the 1Bank Terms and Conditions, and/or any other agreements of the Bank with the Cardholder and/or the holder the Card Account shall apply in relation to the termination of such Terms and Conditions and/or other agreement and/or blocking of the Card, in addition to any rights of the Bank under these Safe@Web Terms.

6.7. If the Cardholder does not accept these Safe@Web Terms and Conditions, he has the right to terminate the Card as described in the Cards Terms and Conditions or the Prepaid Cards Terms and Conditions (as the case may be). Alternatively, the Cardholder may choose not to execute Transactions which require authentication and confirmation via the Safe@Web Service.

7. AMENDMENTS

7.1. The Bank reserves the right to amend these Terms from time to time in the same manner as provided in the Bank's Cards Terms and Conditions and/or Prepaid Cards Terms and Conditions with respect to amendments to the Cards and/or Prepaid Cards Terms and Conditions.

7.2. As soon as the Cardholder receives any notification of any such amendment, he shall notify the contents of the relevant notification and/or the notification itself to the holder of the Card Account. This subparagraph shall apply vice versa also where the holder of the Card Account receives any relevant notification.

7.3 Safe@Web features and functionality may be automatically updated or upgraded without notice to you. At any time, the Bank may decide to expand, reduce, or suspend the type and/or amounts of Transactions authenticated via Safe@Web, or change the Safe@Web procedures. This right to update and upgrade Safe@Web features and functionality will not include changes to your Card(s) or your Card account(s), which will

only be made in accordance with the Cards Terms and Conditions and/or Prepaid Cards Terms and Conditions and/or any other agreements between you and the Bank.

8. WAIVER

8.1 The Bank's failure to exercise or enforce any right or provision of these Safe@Web Terms and Conditions will not constitute a waiver of such right or provision. Any waiver of any provision of these Safe@Web Terms and Conditions and will be effective only if in writing and signed by the Bank.

9. SEVERABILITY

9.1 If any provision of these Safe@Web Terms and Conditions is held to be unlawful, void, invalid or otherwise unenforceable, this shall not affect the validity of any other provision of these Safe@Web Terms and Conditions. In case one or more provisions of these Safe@Web Terms and Conditions are invalid or become invalid as a result of any changing legislation, the validity of the remaining provisions shall not be affected thereby.

10. COMPLAINTS

10.1. The Bank has an internal complaint handling procedure. If you have any complaint about the enforcement of these Safe@Web Terms and Conditions by the Bank, you should follow the relevant complaints procedure as set out in the Cards Terms and Conditions and/or the Prepaid Cards Terms and Conditions, depending on your Card (available on the Bank's website www.bankofcyprus.com).

11. APPLICABLE LAW AND JURISDICTION

11.1. These Safe@Web Terms and Conditions and any amendments to these Safe@Web Terms and Conditions shall be governed by the law of the Republic of Cyprus.

11.2. Any disputes arising from these Safe@Web Terms and Conditions or in connection with these Safe@Web Terms and Conditions that cannot be resolved by means of the internal complaints handling procedure referred to in clause 10of these Safe@Web Terms and Conditions, will be settled by the competent court in the Republic of Cyprus.