TERMS AND CONDITIONS OF eBANKING SERVICE

These Terms and Conditions of eBanking Service ("Terms and Conditions") should be read in conjunction with and constitute an integral part of the agreements and/or the terms for the opening and operation of the Accounts which are governed by these Terms and Conditions. In addition, they should be read in conjunction with the following documents:

- The Framework Contract for Payment Services
- The Commissions and Charges Table of the Bank
- The Cut-off times for Incoming and Outgoing Fund Transfers available on the Banks website at https://www.cdb.com.cy/resources

In the case of conflict between the Terms and Conditions of eBanking Service and one of the abovementioned documents, these Terms and Conditions of eBanking Service will supersede to the extent where they shall not infringe the Law.

1. Definitions and Interpretation

In this document, unless where the text provides a different meaning, the following words will have the below meaning respectively:

Account: means the Account/s held with the Bank at any point in time, in the name of one or more Customers, including Payment Accounts and Card Accounts and which, according to the relevant application and/or notification by the Account Holder/s to the Bank, will be connected via any digital channel, including telephone, internet, telephone application or any other means of communication, which may be specified and provided to the Customer by the Bank from time to time.

Account Holder: means the person, either natural or legal, that maintains an Account with the Bank and has accepted these Terms and Conditions of eBanking Service, by signing the document "Application for eBanking Service" in relation to the services, which are offered by the Bank from time to time.

Account Information Service: means the online service to provide consolidated information on one or more Payment Accounts held by the Payment Service User with either another Payment Service Provider or with more than one Payment Service Providers.

Account Information Service Provider or AISP: means the Payment Service Provider the business activity of which is the provision of Account Information Services.

Authentication Features: means the elements required, or may be requested by the Bank from time to time, for strong Customer authentication purposes, which may concern OTP codes generated throuth the Soft Token, the Hard Token, the SMS Login, or strong Customer authentication codes through Push Notification or other device or application or the Customer's elements categorised as 'inherence'.

Authorised User: means the Account Holder and/or a third person authorised by the Account Holder to have access to any of the services offered by the Bank's eBanking Service.

Bank: means the Cyprus Development Bank Public Company Limited with registration number HE1148 and head offices at 50 Arch. Makarios III Avenue, 1065 Nicosia, Cyprus, as well as its successors, assignees and assignment recipients and which is supervised by the Central Bank of Cyprus.

Business Day: means the day during which the Bank, as the Payment Service Provider of the Payer and/or the Payee, pursues professional activities, as required for the execution of the Payment Transaction.

Subject to the provisions of the Framework Contract it is provided that, the Bank as a Payment Service Provider of the Payer and/or the Payee executes Payment Transactions within Business Days to the extent where such execution is not affected by the official monetary holidays concerning Euro and/or other currencies (as these are determined from time to time by the clearing mechanisms).

Commissions and Charges Table: The table with the charges and/or commissions and/or fees and/or expenses and/or costs and/or payable dues that the Customer must pay to the Bank, as this may be amended from time to time according to the provisions of the Bank's Framework Contract and the Law, and which is available on the official website of the Bank at https://www.cdb.com.cy/client-service-charges and in all of the Bank's branches. The Commissions and Charges Table forms an integral part of the Framework Contract.

Consumer: means a natural person who, in relation to these Terms and Conditions of eBanking Service, is acting for purposes other than his trading, business or professional activity.

Customer: means the person or persons (either legal or natural) and includes Authorised Signatories, who maintain an Account with the Bank.

eBanking Service: means the services offered or that may be offered from time to time by the Bank to the Authorised User and includes, inter alia, the execution of financial and/or banking and other transactions and/or orders and/or instructions and/or the selection of banking or other products and services, via the Bank's web based service, which is accessible via the Bank's Website using the current system and/or any other of its successors or other system that the Bank may use or specify from time to time.

Framework Contract: means the Framework Contract for Payment Services between the Bank and the Customer which governs the execution of individual and successive Payment Transactions and which includes the obligations, the rights and the terms of provision, operation and use of the Payment Account/s.

Law: means the Provision and Use of Payment Services and Access to Payment Systems Law of 2018 (31(I)/2018), as this may be amended or replaced from time to time.

Microenterprise: means an enterprise that at the time of the conclusion of these Terms and Conditions of eBanking Service is an enterprise within the meaning of article 1 and article 2, paragraphs 1 and 3 of the Annex to Recommendation 2003/361/EC, as this may be amended or replaced from time to time. For information purposes only, as at 31/12/2018, a Microenterprise is deemed to be an enterprise that employs fewer than 10 persons and whose annual turnover or the annual balance sheet total does not exceed two (2) million euro.

One Time Passcode or OTP: means the code issued and/or generated by the Security Systems or by any other Payment Instrument of the eBanking Service that may be set by the Bank from time to time.

Password: means the secret alphanumeric code which will be used by the Authorised User together with the User ID and, where applicable, with the Authentication Features that will be requested by him, for access to the Bank's eBanking Service. The Password is issued electronically and is sent to the mobile telephone number which the Authorised User has stated on the "Application for eBanking Service" of the Bank.

Payee: means a natural or legal person that is the final recipient of funds which are the subject of the Payment Transaction.

Payer: means a natural or legal person who holds a Payment Account and allows a Payment Order from that Payment Account, or, where there is no Payment Account, a natural or legal person who gives a Payment Order.

Payment Initiation Service: means the service for the initiation of a Payment Order upon request by the Payment Service User, in relation to a Payment Account held in another Payment Service Provider.

Payment Initiation Service Provider or PISP: means that Payment Service Provider the business activity of which is the provision of Initiation Payment Services.

Payment Instrument: means any personalised device and/or set of procedures agreed between the Customer and the Bank and used in order to initiate a Payment Order, and includes, amongst others, payment cards, the eBanking Service, each of the User ID and Password, Security Systems, OTP, as well as other Authentication Features.

Payment Service: has the same meaning as given to it by the Provision and Use of Payment Services and Access to Payment Systems Law of 2018.

Payment Service Provider or PSP: has the meaning given to it in clauses 4(1), 5(2) and 34 of the Law and includes, amongst others, the Bank, any other bank, or any other licensed payment institutions as defined by the Law.

Payment Transaction: means an act, initiated by the Payer or on his behalf or by the Payee, and which constitutes the placing, transfer or withdrawal of funds, irrespective of any underlying obligations between the Payer and Payee. Payment Transaction does not include any of the payment transactions stated in article 3(3) of the Law.

Payment Order: means every instruction by the Payer or the Payee to his Payment Service Provider requesting the execution of a Payment Transaction. It also includes every instruction transmitted to his Payment Service Provider by a Payment Initiation Service Provider on behalf of the Payer or the Payee.

Reference Exchange Rate: means the exchange rate which is used as the basis to calculate any currency exchange and which is rendered available by the Payment Service Provider or originates from a publicly available source.

Security Systems

(a) SMS Login: means the OTP which is sent via sms to the Authorised User to be used during his first login to the Bank's eBanking Service. It is clarified that, where the Authorised User does not have the Soft Token or the Hard Token, he will then continue to use the SMS Login for his future logins to the eBanking Service.

(b) Soft Token: means the software application downloaded, between others, on the Authorised User's mobile device and/or tablet (provided the said device supports the necessary technology), for OTP generation, for his login and/or for the processing of instructions and/or for confirming the instructions and/or orders and/or for the strong Customer authentication through the Authentication Features, which includes elements that dynamically link the transaction with a specific amount and a specific beneficiary. It is the responsibility of the Authorised User to download the relevant application.

(c) Hard Token Device: means the electronic device provided by the Bank to the Authorised User by completing the relevant application form, which generates OTP to facilitate his login and/or for the processing of instructions and/or orders and/or for confirming the instructions and/or orders and/or for the strong Customer authentication, which includes elements that dynamically link the transaction with a specific amount and a specific beneficiary.

For the acquisition of any of the Security Systems, the Bank is entitled to impose fees as these are listed on the Bank's Commissions and Charges Table, which is available on the website https://www.cdb.com.cy/client-service-charges.

Third Party Providers (TPPs): means the Payment Initiation Service Providers (PISPs) and/or Account Information Service Providers (AISPs) and/or Payment Service Providers issuing card-based Payment Instruments, in each case who have been authorised or registered by the relevant national competent

authority in the EU pursuant to the Law or other law implementing the European Directive 2015/2366 in relation to Payment Services within the internal market.

User ID: means the identification number which is issued by the Bank to the Authorised User, in order for it to be used by the Authorised User together with the Password, and, where applicable, with the Authentication Features that will be requested by him, so that he may have access to the Bank's eBanking Service. The User ID is issued electronically and is sent to the email address which the Authorised User has stated on the "Application for the Use of eBanking Service" of the Bank. It is clarified that the User ID issued by the Bank to an Authorised User for access to his personal Accounts, may be the same with his User ID for access to legal entity Accounts or when he is Authorised to access the Account of another Account Holder.

2. General Terms

2.1 The Bank's eBanking Service is provided to the Account Holder and/or the Authorised User for and on behalf of the Account Holder in accordance with the Framework Contract and (according to the Law) any other such terms and conditions which the Bank may adopt from time to time and which the Bank will communicate to the Account Holder in the way described in clause 15 (Amendments) further below. It is provided that the Account Holder will be responsible for all the acts as well as for any omissions of the Authorised User.

2.2 The following natural persons may have access to and utilise the Bank's eBanking Service:

(i) A natural person who is an Authorised User and

(ii) Has received from the Bank a User ID, a Password and uses one of the Bank's Security Systems.

2.3 The Bank retains the right to reject the application for eBanking Service, in its absolute discretion and without having to justify such a rejection.

2.4 The Account Holder should ensure that the Authorised User accepts and always complies with the Terms and Conditions of eBanking Service. The Authorised User should fully comply at all times with the Terms and Conditions of eBanking Service as well as with all the instructions and/or policies issued by the Bank from time to time in relation to the operation of the eBanking Service.

2.5 The Bank will provide all the required information and will execute instructions given via the eBanking Service of the Bank by the Authorised User, always based on the access rights of each Authorised User, who enters his User ID and Password, and where applicable the OTP and/or any other security password or authentication method or Authentication Features the use of which may be required by the Bank from time to time.

2.6 The provisions defined in these Terms and Conditions of eBanking Service regulate and/or determine the mutual obligations of the Bank and of the Account Holder and of the Authorised User in relation to the transactions of the Account Holder and the of Authorised User via the eBanking Service.

2.7 The Authorised User will ensure that all the instructions given to the Bank are accurate and complete.

3. Security and Limitation of Liability

3.1 Where the Authorised User and/or Account Holder is a Consumer or a Microenterprise, in case he denies having authorised an executed Payment Transaction or he disputes the correct execution of the Payment Transaction, it is for the Bank to prove that the Payment Transaction was authenticated, accurately recorded, entered in the Account held by the Account Holder and

was not affected by a technical breakdown or some other deficiency of the service provided by the Bank.

3.2 The Bank is responsible to the Customer as a Payer for the correct execution of the Payment Transaction, unless the Bank can prove to the Customer that the Payee's Payment Service Provider has received the amount of the Payment Transaction. If the Bank is liable under this clause, for a transaction that was not executed or incorrectly executed, then the Bank, as the case may be, is obliged to refund to the Customer without undue delay the amount of the nonexecuted or incorrectly executed Payment Transaction and, as the case may be, to restore the debited Payment Account to the state in which it would have been had the incorrect Payment Transaction not taken place. When the Payee's Bank is liable based on this clause, it shall immediately make the amount of the Payment Transaction available to the Payee and, as the case may be, credit the equivalent amount to the Payee's Payment Account. In case where the Payment Transaction is executed with delay, the Payee's Bank obtains upon request of the Payer's Bank who acts on the Payer's behalf, that the value date for the Payee's Payment Account is not later than the value date which the amount would have had in case of correct execution of the Payment Transaction.

3.3 It is provided that the provisions of subparagraph 3.2 above do not apply in cases where the Payment Transaction is made and only one of the Payment Service Providers is within the European Union.

3.4 In case of non-execution or incorrect execution of a Payment Transaction, the Bank, irrespective of the liability in the context of this clause, immediately makes effort, if it is requested to do so, to track the Payment Transaction and notifies the Customer for the result, without charging the Customer for this.

3.5 The Bank has the right not to immediately reimburse where there are valid suspicions of fraud or other criminal offences or money laundering offences based on the Prevention and Suppression of Money Laundering and Terrorist Financing Law of 2007, as this may be amended or replaced from time to time.

3.6 The account will not be charged for any damage caused by an unauthorised Payment Transaction, in cases where:

(a) The damage was caused due to the use of the Payment Instrument prior to its receipt and/or activation by the Customer, unless where the said non-receipt and/or non-activation is due to the Customer's failure to notify the Bank for the change of his address,

(b) The Customer has notified the Bank for the loss or theft of the Payment Instrument in accordance with clauses 3.13 (Payment Instrument) and 13 (Communication) as mentioned in the Framework Contract except where he acted fraudulently, or

(c) The Bank failed to provide the appropriate means as in clauses 3.14 (Payment Instrument) and 13 (Communication) as mentioned in the Framework Contract in order to enable the Customer to notify the Bank in relation to the theft or loss of the Payment Instrument, except where he acted fraudulently.

The Bank will bear no responsibility or obligation arising from clauses 3.1 and 3.2 (Bank Obligations) as mentioned in the Framework Contract where the other Payment Service Provider relating to the Payment Transaction is not in a Member State and/or where the Payer is not a Consumer or a Microenterprise.

3.7 It is provided that, if the Payment Order was not executed or was incorrectly executed due to the fact that incorrect/insufficient information was given to the Bank and/or the Unique Identifier required for the correct execution of the Payment Order (as in clauses 2.4.2 (Required information

for a Payment Order) and 2.4.3 (Unique Identifier) of the Framework Contract was incorrect, the provisions of clause 9 (Bank's Obligations) as mentioned in the Framework Contract in relation to the liability of the Bank to reimburse the Customer do not apply.

However, in case of an incorrect execution, the Bank will make reasonable efforts for the recovery of the funds concerning the Payment Transaction. In case where the recovery of the funds is not possible, the Bank shall provide the Customer, upon his written request, all the information available to the Bank, that is important for the Customer, in order to be able to exercise legal action for the recovery of the funds. The Bank may charge for the measures taken regarding the recovery of the funds.

It is provided that the Bank will not be obliged to credit any amount prior to receiving confirmation of the cancellation of the order by an associate or intermediary which the Bank is using for the purposes of effecting the Payment Transaction. It is provided that if the amount of the Payment Order has undergone a currency conversion, the Bank will credit the amount of the Payment Order after it converts it to the initial currency at the prevailing market rate on the date of crediting of the Payer's Account and which is based on the Reference Exchange Rate.

3.8 The Account Holder irrevocably authorises the Bank to accept as duly authorised any instructions given by the Authorised User, given via the eBanking Service of the Bank with the User ID, Password and where applicable the OTP and/or using any other security passwords or devices or Authentication Features which the Bank may require from time to time and which the Bank will communicate to the Account Holder. Its provided that the above will apply based on the access rights as these have been defined by the Account Holder on the relevant application forms. The Account Holder declares, accepts and guarantees that he assumes full responsibility to ensure the Authorised User's compliance with these Terms and Conditions of eBanking Service.

3.9 In order to gain access to the eBanking Service, the Authorised User will enter his User Id, his Password and, where required, the Authentication Features that will be requested by him, as mentioned in these Terms or any other Payment Instrument of the eBanking Service which the Bank may specify from time to time.

3.10 The Authorised User will have to change his initial Password provided by the Bank. In the case where the Authorised User loses the Password, the Authorised User may request a new Password from one of the Bank's business centres or through the eBanking Service. In the case where, the Password is incorrectly entered three times, the User ID of the Authorised User will automatically be locked and may only be restored by contacting the Bank.

3.11 The Bank may, for security reasons, and at any time it may consider necessary, cancel the User ID and/or the Password and/or any security code or device from its records and/or provide the Authorised User with a new User ID and/or Password and/or new security code or device.

3.12 In addition to all other security measures contained in these Terms and Conditions of eBanking Service, the Authorised User undertakes to follow the below security procedures which he recognises as material, for the avoidance of unauthorised access to the Account and/or the Bank's eBanking Service. The Account Holder recognises and agrees that he will be fully liable for any damage that may be caused either to himself, or to the Bank or to any other person as a result of the Authorised User's negligence to comply with the security procedures.

The Authorised User should at all times:

(i) Ensure that all instructions given by himself to the Bank via its eBanking Service are accurate and complete.

(ii) Use exclusively the eBanking Service and always within the available Account limit, which is approved and communicated to the Account Holder and/or the Authorised User by the Bank in the most appropriate method according to the Bank's judgment from time to time.

The Authorised User should not use the eBanking Service to exceed the available Account balance and, where applicable, to exceed the authorisation given to him by the Account Holder.

(iii) Take all necessary measures for the avoidance of the fraudulent use of the User ID, the Password and/or the passcodes generated by the Security Systems.

(iv) Not reveal under any circumstances to any other person, including an employee of the Bank his Password to the Bank's eBanking Service even when requested to do so.

(v) At all times, keep in a safe place and/or under his control, any password or security system, and/or the device used for use of the SMS Login, the Soft Token application or the Hard Token device and/or any other Payment Instruments which the Bank may provide from time to time.

(vi) Delete/destroy from his mobile telephone the message and/or any notification containing his Password and/or the OTP dent to him to be used during his first login and/or when a new Password is sent by the Bank upon his request. Immediately upon receipt, and to never write down or save his Password in any other form. It is provided that the Authorised User will proceed to immediately change his temporary Password upon receipt.

(vii) Avoid selecting a Password which may be easily identified, such as dates of birth, telephone numbers, etc. For increased security purposes, it is deemed appropriate to change the Password on a regular basis.

(viii) Ensure disconnection and deletion of any information from any telephone device, personal computer, or any other equipment used to access the Bank's eBanking Service, prior to leaving the said telephone device, personal computer or equipment unattended.

(ix) Acknowledge his surroundings whilst accessing the Bank's eBanking Service and ensure that he is not being watched or recorded.

(x) Ensure that he is accessing the Bank's eBanking by checking the website's certificate through the browser to ensure it belongs to eBanking and has not expired.

(xi) Ensure there are no monitoring programs being run on his computer since in such a case his User ID, Password, OTP or other Authentication Features or any other security information may be seen or recorded.

(xii) Install an up to date antivirus system and check his computer for viruses on a regular basis.

(xiii) Not open e-mails from unknown senders and delete them without reading their contents in order to avoid the risk of receiving a virus.

(xiv) Never act on the basis of any e-mail, letter or other communication allegedly sent or expressed by the Bank which instructs or encourages him to visit any other site representing that it is another or the new site of the Bank's eBanking Service. The internet site for eBanking is https://ebank.cdb.com.cy.

(xv) Not use any shared computer when accessing the Bank's eBanking Service.

(xvi) Not reveal his User ID or his Password or the OTP to any other person.

(xvii) Never note the Password on anything bearing or which is connected to the User ID or the Hard Token Device or in any comprehensible form or as otherwise may be accessible (one way or another) by a third person.

(xviii) Not allow third persons to watch him whilst typing in his User ID, his Password and the OTP and/or other Authentication Features in order to access the eBanking Service.

(xix) Avoid doing or neglect doing anything within his power, which may allow the inappropriate or unauthorised access or use of the eBanking Service.

(xx) Avoid using an automated connection which stores his Password.

(xxi) Disconnect from the eBanking Service as soon as he is finished. Not to simply close the browser or the application on his mobile phone.

(xxii) Carry the Hard Token Device (if he has one) with him or store it at a secure location where access is controlled.

(xxiii) Avoid login on public wireless networks (especially on those that do not require the use of a password) for purchase processing or access to sites where personal data will be requested by him or information relating to his credentials.

(xxiv) Activate his notifications relating to his transactions.
(xxv) Check regularly the history of transactions of his account.

3.13 The Authorised User should immediately and without delay notify the Bank as provided in subparagraph 3.14(i) of these Terms and Conditions of eBanking Service in the case where he identifies, suspects or realises:

(i) That the User ID and/or the Password and/or the OTP and/or the Authentication Features have been made known to a third person.

(ii) That his mobile phone and/or device and/or any of the security systems that he is using to access the Bank's eBanking Service has been stolen, misappropriated, lost, damaged, misused, or if there is a possibility or suspicion for inappropriate or unauthorised use.

(iii) That his Account has been charged with the amount of a transaction which was executed without his instruction or consent.

(iv) Any error or fault in the operation of anyone of his Accounts with the Bank.

3.14 Without prejudice to the terms and conditions of the Framework Contract, the Account Holder will be fully responsible for all the transactions executed via the Bank's eBanking Service (including any instructions which are given via the Bank's eBanking Service) by the Authorised User. If for any reason the Bank considers that an unauthorised person has used or has attempted to use the Bank's eBanking Service, to intervene in any way in the account of any Account Holder or to give any kind of instruction to the Bank, the Bank may proceed to file a complaint with the police or with any other responsible authority and or reveal any related information to the police or to any other responsible authority without prior notification to the Account Holder and with these terms the Bank is hereby authorised to make such revelations. Irrespective of the above, if the Payment Instrument of the eBanking Service that was issued by the Bank or by a Third Party Provider has been stolen, misappropriated, lost, destroyed, misused, or if an Authorised User knows or suspects that a third person knows or could possibly know the User ID and/or the Password and/or the OTP and/or other Authentications Features, or that any unauthorised transactions took place in the Account or that the access or means of his access to the device which is used for the accessing the Soft Token application or the Hard Token Device may possibly be subjected to or exposed to misuse or abuse, the Authorised User should immediately:

(i) Notify the Bank immediately on 80007979 or on + 357 22 846500 if calling from abroad or visit any of the Bank's business centres (or at any address the Bank may communicate to the Account Holder and/or the Authorised User from time to time as the Bank may deem appropriate). The telephone conversations may be recorded. In the case where the Authorised User notifies the Bank as defined above the User ID, the Password and the registered mobile number will no longer be able to be used for access to the Account via the Bank's eBanking Service directly or via a Third Party Provider (TPP).

(ii) During the Bank's non-working hours (as mentioned on the Bank's website) or during nonBusiness Days, the Authorised User may lock his User ID by incorrectly entering his Password three times.

(iii) Change his Password of the Bank's eBanking Service and communicate with any of the Bank's business centres in order to change his/her registered telephone number if he knows or suspects that they may have been violated.

(iv) Where applicable, to terminate the use of the Security Systems (Soft Token application or Hard Token Device or SMS Login) and apply for a new Security System.

The details contained in such recordings and any other data recordings are considered undisputed evidence and proof to any disagreement.

3.15 The Customer shall bear all the damages relating to the unauthorised Payment Transaction up to the amount of EUR 50 or equivalent amount in any currency (or any other amount that may be determined by the Law from time to time) for the damage resulting from the use of the Payment Instruments that was lost, stolen or misappropriated. This paragraph shall not apply where:

a) the loss, theft or misappropriation of the Payment Instrument was not possible to be detected by the Customer prior to the payment, and provided that the Customer has not acted fraudulently, or

b) the damage was caused by acts or omissions of an employee, agent or branch of the Bank or of an entity to which the Bank's activities were outsourced.

3.16 The Customer is liable for all damages relating to unauthorised Payment Transactions, provided that these were incurred by the Customer acting fraudulently or failing to fulfil one or more of his obligations set out in clause 3 (Security and Limitation of Liability) and/or any clause of these Terms and Conditions intentionally or by being grossly negligent. In such case, the maximum amount referred to in clause 3.15 above shall not apply.

3.17 The Hard Token Device is delivered to the Authorised User personally who, by signing the acknowledgment form, certifies
the physical delivery of the Hard Token Device to him.

3.18 The Account Holder undertakes that both himself and the Authorised User will use at all times such navigation programmes or applications for mobile phones to access the Bank's eBanking Service via the internet as may be specified by the Bank from time to time and will be communicated to the Account Holder in any way the Bank may deem appropriate.

3.19 The Account Holder acknowledges that in the case where he or the Authorised User make use of a different navigation programme to the one specified by the Bank from time to time, all the transactions will be carried out with the sole risk and responsibility of the Account Holder since the Account may be accessible by unauthorised persons.

3.20 The Authorised User and/or Account Holder is obliged to carefully check the balances and statements of his Payment Accounts when such information is made available. In case where the

Authorised User and/or Account Holder finds out that a Payment Transaction has not been executed or has been incorrectly executed or without authorisation, the Account Holder shall be entitled to compensation as described below, provided that he notifies the Bank in one of the ways described in clause 13 (Communication), immediately and without undue delay within a reasonable period of time, which does not exceed thirteen (13) months from the date that the Bank has debited or credited his Payment Account, as the case may be. The Bank will reimburse the Account Holder with the amount of the non-executed or incorrectly executed Payment Transaction or, in case the Account of the Account Holder has been debited, it will restore the debited Account to the state in which it would have been had the payment not taken place, except in cases where irrespective of the currency of the transaction only one of the Payment Service Providers is within the European Union. Where the Account Holder is not a Consumer or a Microenterprise, he is obliged to notify the Bank for a Payment Transaction that was not executed or was incorrectly executed or was executed without authorisation without undue delay and, at the latest, within two (2) months from the date of debit or credit, as the case may be.

3.21 Subject to the provisions of clause 3 (Security and Limitation of Liability) in these Terms and Conditions of eBanking Service, the Bank will be not be in any way responsible to the Authorised User and/or Account Holder for any direct or indirect loss or any other loss of data or loss of gain which may be suffered by the Account Holder or the Authorised User or any other person as a result of unauthorised access to the Account by a third person via the Bank's eBanking Service, due to a fault of his own.

3.22 Furthermore, the Bank will not be responsible for any inaccurate and/or incomplete and/or insufficient information which has been reported/stated by the Account Holder and/or Authorised User via the eBanking Service in relation to the execution of any order and/or transaction. Therefore, the Bank will not be responsible for any damage and/or loss, which the Account Holder and/or Authorised User may suffer as a result of these actions.

3.23 Except as provided by the current Cypriot legislation, the Bank will not be responsible for any loss or damage to the Account Holder or Authorised User or any third person for any unexecuted or incorrectly executed or delayed execution of any transaction, due to electric, electronic, mechanical, communication or similar faults or losses or damages which may result from strikes, war, natural disasters, or any other causes where these are beyond the Bank's reasonable control.

3.24 The Account Holder and/or Authorised User will be responsible and will reimburse the Bank for any loss, damage, cost or fee which the Bank has suffered and/or will suffer in the case where the said loss or damage is the result of any action or omission of the Account Holder and/or Authorised User, or due to a violation of these Terms and Conditions of eBanking Service.

3.25 The Account Holder or the Authorised User must immediately inform the Bank in writing, of any change to his name, nationality, identification documents, address, telephone number (including mobile number) and email address.

3.26 When using the eBanking Service, the Account Holder and the Authorised User will comply with the current legislation and the eBanking Service will not be used for illegal purposes.

3.27 The Bank will have the right to introduce any other additional measures or security procedures and will notify the Account Holder in writing in relation to these.

4. Authorisation and Payment Order Execution

4.1 Where any Payment Orders are being submitted via the Bank's eBanking Service, the provisions stated in the Framework Contract will apply.

4.2 The Authorised User authorises and instructs the Bank to act in accordance with all the instructions for the execution of transactions which are received via the eBanking Service or Third Party Provider (TPP) acting on behalf of the Authorised User and/or Account Holder, provided that such instructions are validated as authorised by the Account Holder and/or the Authorised User in accordance with these Terms and Conditions of eBanking Service and/or with the authorisation procedures of the TPP.

4.3 In case of Accounts which operate with a multiple signature scheme, the Bank shall consider an order as authorised by the Authorised User provided that the User Id, the Password and, where required, the OTP generated by the Security Systems or any other Payment Instrument of the eBanking Service or other Authentication Features which the Bank may specify and/or request from time to time, have been provided by all authorised signatories.

4.4 In the case where the Authorise User initiates a Payment Order via a PISP, he should comply with the authorisation procedures, which have been agreed with the particular PISP.

4.5 The Bank assumes responsibility for the correct and timely execution of the Payment Orders which have been given by the Authorised User, as soon as these have been received by the Bank's systems, in accordance with the Framework Contract.

4.6 The Bank reserves the right to delay any execution or not to execute any Payment Orders if these Payment Orders exceed the internal security limits set by the Bank, and/or the regulations imposed by any related legislation, which aim to protect the security interests of the Authorised User and/or the Bank and in such a case the Authorised User will be notified in any way the Bank may deem appropriate as to the fact that his instructions have not been executed.

4.7 In the case of non-execution of a Payment Order or future payment instruction, due to lack of funds in the account or for any other reason, the Bank may make available to the Authorised User information relating to the non-execution of the Payment Order.

4.8 The daily limits for performing transactions are set during the application process for access to the eBanking Service. The Account Holder may apply for amendments to these limits.

4.9 The Bank may specify maximum transaction limits and/or any other limits in relation to the Accounts and/or in relation to the Payment Orders and/or certification of the authenticity and/or Payment Instruments and/or access method. These limits may be constructed in accordance with the value of the transactions and/or the volume of the transactions and/or the time period and/or the type of transactions or in accordance with any other metric that the Bank may decide, in its absolute discretion. In the case where the Payment Order exceeds any of the Bank's limits then the Bank may refuse to proceed with execution.

4.10 In the case of fund transfer orders in foreign currency, the exchange rate, which will be used for the transaction, will be the exchange rate applicable on execution date.

4.11 Except as provided by the current legislation, the Bank bears no responsibility for any delay during the processing or execution of any instructions which are given by the Authorised User as mentioned above or otherwise, if the delay has been caused due a possible malfunction operation of the telephone network, which does not fall under its jurisdiction or control and may have a negative effect in the correct and timely execution of instructions.

5. Revocation of Payment Orders

5.1 The Customer is not allowed to revoke a Payment Order once it has been received by the Bank, unless otherwise explicitly mentioned.

5.2 In case where a Payment Order is initiated by a Payment Initiation Service Provider, the Customer cannot revoke it after providing his consent to the Payment Initiation Service Provider to initiate the Payment Transaction.

5.3 In case of agreement for the execution of a Payment Order on a certain date or at the end of a certain period or on the date where the Payer will have made funds available to the Bank, the Payer may revoke the Payment Order the latest until the end of the Business Day preceding the agreed day.

5.4 After the time frames set in clause 5.3 above have elapsed, the Payment Order may be revoked only upon agreement between the Customer and the Bank.

5.5 In case of revocation of a Payment Order, the Bank has the right to impose charges, according to the Commissions and Charges Table.

5.6 An application for the revocation of a Payment Order must be authorised by the Customer in one of the ways described in the Framework Contract, depending on the case.

Where the Customer is neither a Consumer nor a Microenterprise, the Bank may, but is not obliged, to accept revocation of the authorisation.

6. Time of Receipt of Payment Order and cut-off times

6.1 Time of Receipt of Payment Order means the time that the Bank receives the Payment Order, indirectly or directly. In case the Payment Order is received by the Bank on a non-Business Day, or it is received on a Business Day but after the cut-off time, then it will be deemed to have been received on the next Business Day. The cut-off time may differ according to the Payment Transaction, the currency in which it will be executed or other parameters, which the Bank may specify from time to time. Information in relation to the cut-off times are available on the Bank's official website at https://www.cdb.com.cy/resources, as well as at any of the Bank's branches.

6.2 The Bank reserves the right to extent its cut-off time, without prior notice to the Customer and to execute Payment Orders even though they have been received after the set cut-off time.

6.3 In case of an agreement that the execution of the Payment Order begins on a specific day or at the end of a specific period or on the day on which the Payer will make the funds available to the Bank, the agreed time will be deemed to be the Time of Receipt of the Payment Order. If a nonBusiness Day was agreed, then the Payment Order shall be deemed to have been received on the next Business Day.

6.4 It is provided that in case where the Payer does not define the date on which he wishes his Payment Order to be executed, the Bank shall have the right to execute it immediately.

6.5 The time of receipt of the Payment Order via eBanking, which is received prior to the Cut-off time, will be considered to be the time during which the Bank receives the order for the execution of the Payment Transaction which is transmitted directly by the Authorised User or any Third Party Provider (TPP) authorised for this purpose by the Authorised User and/or the Account Holder. Where the time of receipt is after the cut-off time of the relevant particular Service, the Payment Order will be considered to have been received the next Business Day.

6.6 The Account Holder and/or the Authorised User will be responsible towards the Bank for all the Payment Transactions effected via the eBanking Service and/or, where applicable, through the use of the services of a Third Party Provider (TPP), as well as for all the acts and omissions of the Account Holder and/or Authorised User and will authorise the Bank to execute all the Payment Transactions by debiting the Account.

7. Updates and Correctness of Information

7.1 The Authorised User may be informed of the Account balance and/or Payment Transactions, which are made to and from the Account either via the Bank's eBanking Service and/or at any of the Bank's business centres and/or via any other means which the Bank may provide from time to time.

7.2 The Bank's eBanking Service allows Account updates in real time. Despite this fact, the time required to complete the processing of instructions may differ according to their nature and to whether processing is carried out immediately. As a result, the Authorised User recognises and accepts that the information related to the Account balance and the transactions via the Bank's eBanking Service are as updated as the Bank's systems allow at the time of the inquiry, however they may possibly not include current transactions which have not been processed or authorised.

7.3 The Bank will make every reasonable effort in order to ensure correctness of any information received by the Authorised User via the Bank's eBanking Service but, with the exception of any possible provisions in the current legislation to the contrary, the Bank will not be responsible for the correctness of the said information or for any loss, direct or indirect, which the Account Holder may suffer or any other third person when the information is inaccurate or not updated.

8. Limitation of Access to the eBanking Service and Termination

8.1 The Bank may terminate and/or block and/or limit and/or deny access to the Bank's eBanking Service where the Bank has reasonable suspicion that it is related with:

(i) The security of the Bank's eBanking Service and/or the User ID and/or the Password and/or the OTP and/or other Authentication Features or

(ii) The unauthorised or fraudulent use of the Bank's eBanking Service and/or the User ID and/or the Password and/or the OTP and/or other Authentication Features.

(iii) The possibility of insolvency of the Account Holder.

(iv) And where the Bank has an obligation to act accordingly based on any legislation or upon request by any supervisory authority.

8.2 The Bank will notify the Account Holder in any way it considers appropriate in relation to the termination and/or blocking and/or limitation and/or refusal of his access to the Bank's eBanking Service and the reasons for this decision taken by the Bank. Where possible, the above information will be given by the Bank to the Authorised User prior to the blocking or, where this is not possible, immediately thereafter. The Bank will have no obligation to provide the abovementioned information unless providing such information would compromise objectively justified security reasons or is prohibited by any provision of another relevant Cypriot or Community legislation.

8.3 The Bank will unblock the Payment Instrument of the eBanking Service or replace it with a new Payment Instrument, once the reasons for the blocking no longer exist.

8.4 The Bank may from time to time and in its absolute judgement delay and/or suspend and/or terminate and/or deny the execution of any order and/or transaction pending completion of all necessary and/or required checks in relation to compliance matters and/or money laundering and/or financial fraud and/or legislation. The Bank will notify the Authorised User and/or Account Holder, in any way it deems to be appropriate. The Bank will have no obligation to give such notice if it is against any objectively justified security reasons or is prohibited by any provision of another relevant Cypriot or Community legislation.

8.5 Furthermore, the Bank provides information electronically in relation to the status and/or the processing stage of any order and/or transaction via the eBanking Service. It is important that the Account Holder and/or the Authorised User checks carefully and regularly the status and/or processing stage of any order and/or transaction, through the electronic information provided by the eBanking Service and where any questions arise in relation to the delay and/or suspension and/or termination and/or refusal, the Account Holder and/or Authorised User should communicate directly with the Bank at the address and/or telephone number stated in clause 13 (Communication).

8.6 The Bank shall bear no responsibility for any damage and/or loss suffered by the Account Holder and/or the Authorised User as a result of the delay and/or suspension and/or termination and/or refusal to execute any order and/or transaction for the reasons mentioned above.

8.7 The Account Holder may terminate the agreement for the provision of the eBanking Service by giving a written notice of termination to the Bank, at least one (1) month in advance. In the case where the Customer, being a Consumer or Microenterprise, terminates the agreement for the provision of the eBanking Service within six (6) months from the date it has been concluded, the Bank retains the right to apply a charge in accordance with the Bank's Commissions and Charges Table. Where the Customer is neither a Consumer not a Microenterprise, the Bank may apply a charge for the termination of the agreement for the provision of the eBanking Service at any time. The said charge will be imposed in accordance with the Bank's Commissions and Charges Table.

8.8 The Bank retains the right to suspend the operation of the eBanking Service and to notify the Account Holder and/or Authorised User by any means the Bank deems appropriate.

8.9 The services offered by the eBanking Service may be restricted by the Account Holder in relation to the Authorised User, given that the relevant written instructions are submitted to the Bank by the Account Holder and provided that the Bank will confirm receipt of these instructions.

9. Alerts Service - Text Alerts (sms) or Email Alerts

9.1 The Alerts Service is a service which is offered by the Bank's eBanking Service which sends notifications to the registered mobile number or the email address of the Authorised User containing information. This service provides security to the Authorised User in the case of fraudulent or unauthorised use of his security passwords, in relation to the services offered by the Bank. For some transactions which are executed by the Authorised User e.g. Login to the eBanking Service, the Alerts Service is not possible to be cancelled by the Authorised User. In some cases, the Authorised User, however, may differentiate the method of receipt of the alerts so as they are received via email at his registered email address.

9.2 The Account Holder acknowledges and accepts that the Bank:

(i) Is not and will not be responsible or accountable for the deletion, partial deletion or inability to transmit any messages.

(ii) Does not guarantee that the Alerts Service will be continuous, timely, secure or without errors or that the Alerts Service will be available at any particular time or place.

(iii) Will not be in any way responsible for any loss or damage of any kind suffered by the Authorised User and/or Account Holder and/or third persons as a result of the content transmitted via the Alerts Service.

(iv) In the case where the Authorised User registers with the Bank a mobile number and/or email address besides his own, the Bank will not be in any way responsible for any damage, loss or difficulty suffered by the person to whom the Alerts Service notifications will be transmitted.

In the case where the said person claims compensation from the Bank to this regard, the Account Holder will compensate the Bank fully.

9.3 Any Notification of the Alerts Service will be transmitted only once. In the case where the receiver deletes the message, the Bank does not have the ability to resend the message.

10. Intellectual Property Rights

The use of the Bank's eBanking Service by the Account Holder and/or the Authorised User does not give them any rights to the Bank's intellectual property, whose legal owner is the Bank itself. Any copying or distribution or transmission or broadcast in any electronic or other means or adaptation or modification or readjustment of any material of the Bank's eBanking Service is strictly forbidden.

11. Joint Accounts

Without prejudice to any instructions or orders for the operation of the Joint Account held with the Bank by two or more persons (from now on the "Joint Account") the Joint Account co-holders may authorise any person, including one of the Account Holders of the Joint Account, to be an eBanking Authorised User, provided that all the other co-holders of the Joint Account have given their consent in relation to this action.

12. Death or Incapacity of the Authorised User and/or Account Holder

In the case of death or incapacity of the Account Holder and/or the Authorised User, the Bank will have the right to provide all the information requested and to execute all the instructions given via the Bank's eBanking Service της Τράπεζας with the use of the User ID, the Password and/or the OTP until the said death or incapacity is brought to the attention of the Bank, and is confirmed by the Bank.

13. Communication

13.1 Any notification should be written and delivered or sent by the Customer to the Bank:

(i) At Alpha House, 50 Archbishop Makarios III Avenue, 1065 Nicosia

(ii) At the Bank's postal address P.O. Box 21415 CY-1508

In the case of need for direct communication with the Bank or for obtaining further clarification you may contact us by telephone on 80007979 or + 357 22 846500 if calling from abroad during the Bank's working hours.

13.2 The Bank will communicate with the Customer at his last known correspondence and email address and the date of communication will be considered as the date of its dispatch.

13.3 The Customer is obliged to immediately notify the Bank of any changes to his contact details in accordance with clause 3.25.

13.4 The Bank shall have no liability or obligation for any damage or loss which may be caused to the Customer as a result of any delay, misunderstanding, destruction, or other irregularity to the dispatch of any notice through any communication method stated above either to or from the Customer, or to any third person, for reasons outside the Bank's control.

13.5 Telephone conversations through number 80007979 or + 357 22 846500 may be recorded and may be checked and maintained for any time period as specified by the Bank from time to time. The Customer accepts that any such recordings may be used as proof, to the point considered necessary or appropriate, in the case of dispute.

14. Miscellaneous provisions

14.1 Any omissions on the part of the Bank to exercise its rights based on any clause of these Terms and Conditions of the eBanking Service will not be considered as waiving of the Bank's rights.

14.2 These Terms and Conditions of eBanking Service will be in Greek and/or English, according to the Customer's choice and will be of indefinite duration.

15. Amendments

15.1 The Terms and Conditions of eBanking Service may be amended at any time and the Bank shall notify the Customer of such amendments through announcement and/or publication on the Bank's website at http:/www.cdb.com.cy/ and/or through publication to the press and/or by any manner that the Bank may deem appropriate.

15.2 If the Customer is a Consumer or a Microenterprise, the Bank shall inform the Customer about every amendment of these Terms and Conditions at least two (2) months prior to the proposed effective date of the amendment, by post and/or by any other means as the Bank may consider to be effective notice to the Customer.

15.3 If the Customer is neither a Consumer nor a Microenterprise, any amendment may take effect without prior notice.

15.4 Amendments, which are more favourable to the Customer, may be applied without notice.

For any amendments not relevant to the Payment Services, if the amendment is to the benefit of the Authorised User and/or Account Holder the amendment will be put in immediate effect and the Authorised User and/or Account Holder will receive notice within 30 days. Where the amendment is neither to the benefit nor the loss of the Authorised User and/or Account Holder, the Bank will give at least 30 days advance notice prior to effecting the amendment. Where the amendment is to the detriment of the Authorised User and/or the Account Holder, the Bank will give at least 60 days advance notice prior to effecting the amendment.

15.5 Irrespective of the above, as soon as the Authorised User receives any kind of notification in relation to the modification of these Terms and Conditions, he will be obliged to disclose the content of the relevant notification and/or the notification itself to the Account Holder. This subparagraph will apply vice versa in the case where the relevant notification is received by the Account Holder.

15.6 The Account Holder shall be deemed to have accepted the proposed by the Bank changes, unless he notifies the Bank that these are not accepted prior to the proposed date of entry into force of the amendment. Where the Account Holder does not accept the amendment, he has the right to terminate the use of the eBanking Service immediately, by informing the Bank, free of charge, and prior to the suggested effective date of the amendment, in accordance with the provisions of these Terms and Conditions and in particular clause 13.1 above. Where the Account Holder does not accept the amendment, he has the right to terminate his authorisation immediately, by informing the Bank in writing, free of charge, and prior to the suggested effective date of the amendment, in accordance with to the provisions of these Terms and Conditions and in particular clause 13.1 above. Where the Authorised User does not accept the amendment, has the right to terminate/recall immediately the authorisation given to him by informing the eBanking Service in writing, free of charge, and prior to the suggested effective date of the amendment, in accordance with the provisions of these Terms and Conditions and in particular clause 13.1 above.

16. Jurisdiction

The laws of the Republic of Cyprus will govern these Terms and Conditions and its courts of justice will have jurisdiction to resolve any difference which may occur by or in relation to them.

It is provided that this clause will not limit the Bank's rights to exercise legal measures in any other court of justice abroad which have jurisdiction as well as to register and execute any decision which is taken in Cypriot courts of justice in relation to any property which belongs to the Customer or to any claim by the Customer in any other country.

17. Acceptance

These Terms and Conditions shall be deemed as accepted by the Customer upon entering his or his authorised representative's signature on the Bank's application. Where the Customer is a legal entity, it should also submit the following:

- Board resolution for the acceptance of these Terms and Conditions and authorisation of the person entitled to sign this agreement on its behalf
- The "Consent and Acknowledgement Form" signed by the Authorised User.

18. Customer Declaration

The Customer declares that he fully understands his right to review these Terms and Conditions with a lawyer of his choice, that he had the opportunity to consult a lawyer of his choice, and that he freely and consciously enters into the agreement and provides his consent to these Terms and Conditions.

19. Information Disclosure and Disclosure to Third Party Providers (TPPs)

19.1 These Terms and Conditions include the agreement between the Bank and its customers who are using the eBanking Service. For the purpose of the provision of the agreed services, the Bank and the companies of its group are processing information relating to the Customer and its affairs and the said processing is carried out discreetly and based on Cypriot law.

19.2 These Terms and Conditions of eBanking Service should be read in conjunction with the Bank's Privacy Statement, which is available at https://www.cdb.com.cy/privacy-policy (the "Privacy Statement"). The Privacy Statement sets out detailed information about the Bank's use of Personal Data. The Authorised User and/or Account Holder and any co-holder of the Account should review this Privacy Statement to ensure that he understands how the Bank processes his Personal Data and understands his relevant rights.

19.3 Where the Authorised User and/or Account Holder enters into a contractual relationship with a Third Party Provider (TPP) and/or allows a Third Party Provider (TPP) to access information in relation to an Account or to carry out a Payment Transaction for him from the Account and/or in general uses the services of a Third Party Provider (TPP), the Authorised User and/or the Account Holder and or any co-holder of the Account agrees that the Bank shall disclose to that Third Party Provider (TPP), account information and/or grant the TPP access to the Account Holder's Account(s) to the extent requested by the Authorised User and/or Account Holder, provided that:

(i) Such Third Party Provider (TPP), is authorised or registered by the national competent authority in the EU pursuant to the Law, or such other national implementing legislation in respect of Directive (EU) 2015/2366; and

(ii) The Account Holder has given his explicit consent to the Bank to meet such a request by Third Party Provider (TPP), or has explicitly authorised the Authorised User to give his consent and the Authorised User has indeed given this consent; and

(iii) The Bank discloses such information and/or grants such access subject to any limitations that the Account Holder or the Authorised User, where applicable, has brought to the attention of the Bank; and

(iv) The Account Holder's and/or the Authorised User's and/or Third Party Provider's (TPP) request, is made in accordance with the Law and any other applicable law; and

(v) The Bank and/or any other relevant authority has not blocked the access of such Third Party Provider (TPP) due to violation by such Third Party Provider (TPP) of any applicable law and/or where there are concerns that it is acting on an unauthorised or fraudulent basis and/or it does not meet the required security measures and standards. In that case, the Bank will confirm to the Customer its refusal unless doing so would compromise reasonable security measures and/or any applicable national or European law.

Where the Account Holder and/or the Authorised User are provided with a card-based Payment Instrument by a Third Party Provider (TPP) which is linked to an Account which is accessible online, the card-based Payment Instrument issuer may request confirmation from the Bank that the amount necessary to execute the card-based Payment Transaction is available in the Account Holder's Account. The Authorised User and/or Account Holder agrees that the Bank may provide this confirmation in the form of a simple "Yes" or "No" communication immediately in response to such request.

19.4 For the avoidance of doubt, clause 19.3 applies also to joint Accounts. The co-holders of such joint Accounts hereby give their explicit consent to be bound by the actions and/or decisions of the Account Holder and/or Authorised User in authorising the Bank to disclose to a TPP any Account Information and/or to enable access to the Account(s) as described in clause 19.3.

19.5 To revoke the authorisation given under clause 19.3 and 19.4, the Authorised User and/or Account Holder shall inform the Bank through his access to the eBanking Service. It is provided that the above will be put in effect according to the access rights as these have been submitted by the Account Holder on the relevant applications.

20. Commissions and Charges

The Bank will have the right to apply commissions and/or charges for the execution of a Payment Transaction through the eBanking Service and/or through the use of the services of a Third Party Provider (TPP), as explained in clause 19.3. και 19.4, in accordance with the Commissions and Charges Table in effect at the time of execution, as may be amended from time to time, which will be provided to the Authorised User and/or Account Holder and will be available to the Authorised User and/or Account Holder at the Bank's branches as well as on the internet on the website https://www.cdb.com.cy/.

21. Gender and Number

Any reference in this Framework Contract in the male gender shall also include the female and vice versa and any reference to singular number shall also include plural number and vice versa.