BEA東亞銀行

UK Corporate Cyberbanking Service Terms and Conditions

1. Introduction

1.1 This document sets out the terms and conditions that apply to the use of the UK Corporate Cyberbanking Service (the "**Service**"). These terms and conditions apply in addition to our General Terms and Conditions and Products Terms and Conditions (copies can be obtained from our website or in branch) for the Account or the service that are accessible via the Service and our General Terms and Conditions are accordingly incorporated herein. In the event of any inconsistency between our General Terms and Conditions and Products Terms and Conditions, in relation to the use of the Service, the terms and conditions set out herein will prevail. Please read these terms and conditions carefully before using the Service.

2. Definition

2.1 "**Account**" means a corporate account with us that is accessible via the Services;
2.2 "**Administrator**" means any person designated by the Customer to act on behalf of the Customer (including without limitation by designating Approvers) and to be responsible for the management and control of the use of the Service from time to time;
2.3 "**Approval Arrangement**" means the number of Approvers (one or more) for approving transactions required by the Bank from time to time;
2.4 "**Approver**" means a person designated by an Administrator to authorise instructions to the Bank submitted using the Service by an Inputter for and on behalf of the Customer;
2.5 "**Bank**" (also "**we**", "**us**" and "**our**") means The Bank of East Asia Limited, acting through its UK branch ("BEAUK") with its registered address located at 75 Shaftesbury Avenue, London W1D 5BB;
2.6 "**Browser**" means any Internet browser supported by the Service;
2.7 "**Business Day**" means any day (excluding Saturdays, Sundays and bank holidays in England) that we are open for the transaction of normal banking business;
2.8 "**BEA UK App**" or "**App**" means the BEAUK mobile application provided by BEAUK for generating a Security Code using the i-Token Service and accessing other information relating to BEAUK and the services provided by BEAUK;
2.9 "**Corporate Cyberbanking Service**" or "**Service**" means the internet banking service that we make available from time to time through the Internet to enable the electronic receipt and transmission of information (including in relation to an Account);
2.10 "**Customer**" (also "you", "your" and "yours") means any sole proprietorship, partnership or corporation who applies for the Service and whose application is accepted by the Bank;
2.11 "**Cut-Off Time**" means the time of a Business Day that we must receive Instructions by if they are to be processed on the same Business Day;
2.12 "**Cyberbanking Number**" means the unique identifier allowing a User to access and use the Service;
2.13 "**Enquirer**" means a person designated by an Administrator to make enquiry of the Account and any other information available via the Service for and on behalf of the Customer;
2.14 "**Inputter**" means a person designated by an Administrator to input instructions to the Bank for and on behalf of the Customer using the Service;
2.15 "**Instruction**" means, with respect to an Account, any request given by the Customer, an Administrator or any User for a deposit, withdrawal, transfer, payment, access to Account status, balances or access to any other Account information that we make available;
2.16 "**i-Token**" means a device binding unique identifier which could be downloaded to the User BEA UK App and stored in the keychain (or other security area described by the

Bank from time to time) of the designated mobile device after successful registration of i-Token Service;

2.17 "**i-Token Service**" means the service provided by the Bank to the User from time to time in relation to i-Token as alternative two-factor authentication method, which enables the User to use i-Token PIN/biometric authentication to login/confirm transactions performed in the Corporate Cyberbanking Service via the designated mobile device;

2.18 "**i-Token PIN**" means the alphanumeric code created by the User during the enrolment for the use of i-Token Service;

2.19 "**Limit**" means any transactional, daily or other limit on the amount that may be paid, transferred or withdrawn in a transaction or series of transactions using the Service;

2.20 "**One Time Password (OTP)**" means the unique code that can only be used once and is sent to the User registered mobile phone number by the Bank via Short Message Service ("SMS") to access the Service;

2.21 "**Personal Identification Number (PIN)**" means the code issued to a User by the Bank or chosen by the User to access the Service;

2.22 "**Security Details**" means the Cyberbanking Number, PIN, OTP and any other identification or secret code assigned for the authentication of the User by the Bank from time to time;

2.23 "**Security Code**" means a one-time numerical code generated through i-Token Service to login and/or confirm transactions performed via the Service;

2.24 "**User**" means an Administrator, Enquirer, Inputter or Approver; and

2.25 "**Website**" means the website designated by the Bank from time to time through which Users can access the Service which at the present is at www.hkbea.co.uk.

3. Use of the Service

3.1 The Corporate Cyberbanking Service enables the Customer to carry out certain banking functions in the Accounts that you have with us. By using the Corporate Cyberbanking Service, you accept these terms and conditions. You are strongly advised to read the terms and conditions before using the Corporate Cyberbanking Service.

3.2 The Customer is only permitted to use the Service in accordance with these terms and conditions, and in accordance with our instructions which may be provided by us at any time by any method of communication agreed between us and the Customer.

3.3 All Accounts and payee templates that you have registered will be accessible via the UK Corporate Cyberbanking Service.

3.4 In order for us to act on you Instruction submitted using the Services, you must provide us with the same information onscreen as you would when placing such an Instruction in-branch. The required information is set out in the General Terms and Conditions for the relevant Account

3.5 Each time when accessing the Service, the User will be asked to input the Security Details. The Security Details requested, for example, your Cyberbanking number (in relation to the UK Corporate Cyberbanking Service only), PIN and Security Code generated through i-Token Service (where relevant), may differ whether you have entirolled in the i-Token Service. Your inputting of the correct Security Details will act as your consent to us executing the Instructuion(s) submitted via the Services.

3.6 If the User did not enrol for i-Token Service, the User will continue to receive OTP when accessing the Service. The OTP is sent to the User's registered mobile phone number as an additional level security. The services accessible via i-Token or OTP may not be the same.

3.7 Customers shall designate and appoint one or more Administrators to give instructions to the Bank relating to the access and the use of the Service on behalf of the Customer. The Instructions given by an Administrator shall be binding upon the Customer. An Administrator shall manage and control the access and use of the Service including without limitation the designation of Users (determining which individuals have access to which functionality within the Service) and the distribution of PINs to Users pursuant to these terms and conditions.

3.8 Where relevant, the Administrator shall collect the Security Details for the Service from the Bank or the Bank shall deliver the Security Details for the Services to the Administrator using the address in the Bank's record and the Administrator shall pass the relevant Security Details to the relevant Users. The Customer shall and shall ensure that each Administrator and each other User shall keep the Security Details secure and the Customer shall be fully liable and responsible for any loss, claim, damage, cost or expense whatsoever and howsoever suffered or incurred by any person arising from or in connection with any breach of these terms, negligence, improper use, misuse, theft or loss of the Security Details.

3.9 We may require the Customer, User and other personnel of the Customer to visit one of our branches in person in relation to the Service for identification and other checks that may be required from time to time according to our procedures for the operation of the Service.

3.10 By using the Service, the Customer accept(s) these terms and conditions.

3.11 The Bank shall use all reasonable endeavours to ensure that information made available by the Services are correct and updated at regular intervals. The transaction details and Account balances as shown via the Services are for reference only. Those transaction details and Account balances as recorded in our internal banking systems rather than as shown on the Services will be conclusive evidence as to the transactions and balances.

4. Security

4.1 The Customer acknowledges and agrees that it has a duty of care to us to ensure the competency, honesty, integrity and suitability of all Users.

4.2 The Customer shall and shall ensure that each User observes and complies with the bank security precautions. Security tips and FAQ are available when logging in to the Service and on our website. This would include:

- Keeping vigilant at all times and avoiding clicking on embedded hyperlinks in any communication received from us that the User has reason to believe may be suspicious;
- Never disclosing login information needed to utilise the Service to a third party;
- Regularly ensuring information with us is up to date, and changing passwords regularly; and
- Only logging into the Account by typing www.hkbea.co.uk into your web browser.

4.3 The Customer undertakes to check the Account balances and transactions regularly. If the Customer suspects or has become aware or the loss, theft, misappropriation or any unauthorised access to the Account (including any unauthorised or incorrectly initiated or executed payment transaction) via the Service , the Customer should notify us immediately.

4.4 If the User choose to use fingerprint or any other means of biometric identification to generate the Security code, then the Customer/User agree that these forms of authentication can be used to log in to and confirm certain transactions in the Services. User should not allow anyone else's fingerprint or other biometric means of identification to be stored on the device as that fingerprint or other biometric identification can be used to access the Services.

4.5 If any Security Details are entered incorrectly several times, the Service will be suspended for that User and the individual will have to re-register through the UK Corporate Cyberbanking Service in order to continue to use the Service.

4.6 In the event of suspected or actual fraud or a security threat, we will contact you via the User's registered phone number and e-mail address, providing the individual with details of the activity itself and measures we are taking to protect the Account.

4.7 We reserve the right to refuse any Instruction if we have reasonable grounds to believe that:

- The security of the Service has been compromised;
- There is suspected unauthorised or fraudulent use of the Service; or

- in the event that the Account offers an overdraft facility, a significantly increased risk that the Customer may be unable to fulfil its liability to pay.

4.8 If any of the circumstances in Clause 4.7 occur, we will inform the User that we intend to stop usage of the Service in the manner they have been used, and provide reasons for this. If we are unable to provide reasons why such usage is stopped in real time because it would compromise security measures, or we are unable to due to law or regulatory reasons, we will inform the User of this as soon as reasonably practicable.

4.9 If the above occurs, we will allow the Service to resume as soon as the circumstances detailed in Clause 4.7 cease to exist, or if permitted, provide the User with new Security Details so that Services can be accessed as soon as possible.

4.10 For more information on all types of fraud and how to prevent becoming a victim, please visit the government website at http://www.moneyadviceservice.org.uk.

4.11 We shall not in any event be liable for any loss or damage whatsoever suffered by the Customer as a consequence of the User's failure to observe and comply with any of the above security precautions.

4.12 Where your Security Details are used without authority by someone else other than you, you may be liable for a portion of the losses from your Account before applying the refund. However, this will not apply if:

(a) the loss, theft or misappropriation of the Security Details was not detectable prior to the payment, save where the User or Customer have acted fraudulently;
(b) such loss occurs before the Security Details have been received or set up;
(c) such use occurs after the User has notified us that your Security Details have been lost, stolen or used without authorisation;
(d) we have failed to tell the User how to notify us of any loss, theft or unauthorised use of the Security Details;
(e) we do not apply procedures that we are legally required to use to check a payment has been authorised by the User; or
(f) the loss was caused by acts or omissions of an employee, agent or branch or of an entity carrying out activities on behalf of the Bank.

4.13 However, clause 4.12 (a – f) will not apply and the Customer will be responsible for the full amount of the Transaction if:

(a) the User or Customer authorised the Transaction;
(b) the User or Customer agreed to provide the Security Details to another person;
(c) the User or Customer failed to use your Security Details in accordance with these terms and conditions;
(d) the User or Customer failed to notify us in the agreed manner and without undue delay on becoming aware of the loss, theft or misappropriation of your Security Details; or
(e) the User or Customer has acted fraudulently.

5. Accessing and using i-Token on the BEA UK App

5.1 i-Token is built into the BEA UK app which provides an alternative means of authentication for using the Service. Where the Customer wish to use i-Token, each User must enrol the use of the i-Token Service on the BEA UK App on their device. This is carried out by completing the registration steps specified by the Bank. Once successfully registered, the User will be asked to create an i-Token PIN. The User may then use i-Token PIN/ fingerprint recognition or other biometric means of identification that may be allowed on their device to generate a Security Code for login/ confirm transactions in Service.

5.2 If the User changes device, or wish to enrol i-Token on a different device, the User should follow the installation and activation procedures of i-Token as prescribed by the Bank.

5.3 i-Token can only be active on one device for each User, but may be used in respect of the Service for multiple Accounts. Any existing i-Token of a User will be deactivated after a new i-Token is successfully registered on a different device for that User .

5.4 A User will need access to the internet to enrol the use of i-Token. Once successfully registered, a Security Code can be generated afterward without internet access.

6. Support for the BEA UK App

6.1 In order to use the BEA UK App the User must have a compatible device running a compatible version of the operating system.

6.2 A User may not be able to use the BEA UK App until latest software updates are downloaded and any new terms are accepted.

6.3 We may periodically issue updates to the BEA UK App through the Apple App Store or Google Play. User must download these updates and User should regularly check for updates as User may not be able to use the BEA UK App until they have been downloaded. Apple is a trademark of Apple Inc. Google Play is a trade mark of Google Inc.

6.4 We may stop supporting the BEA UK App on the User device or on the version of the operating system running on the User device. When it happens, the User will no longer be able to use the BEA UK App until the user has obtained a new device which is supported or updated the operating system on that device, as applicable.

6.5 User will need access to the internet to use the BEA UK App.

7. Acting on the Customer's Instructions

7.1 All authorised Instructions, once received, shall be irrevocable and binding on the Customer. The Bank's record of Instructions and transactions shall be deemed to be conclusive evidence against the Customer.

7.2 Any Instruction given to the Bank via the Service shall operate as request by the Customer to the Bank to act on the Instruction. Where an Instruction relates to a payment or a transfer, please refer to our General Terms and Conditions in particular to understand how it will be effected. The User authorises us to accept and act on the Instruction we receive through the Service. We will not make any further enquiries into the authenticity of an Instruction.

7.3 If an Approver has enrolled for the i-Token Service, the Approver is permitted to add or manage payees for Instructions online using the Service without any additional approval formalities within the Service. If no Approvers have enrolled for the i-Token Service, only the Administrator will possess the ability to add or manage payees, through the submission of a [Cyberbanking form]. A payee must be added using this process before any Instruction can be made in respect of that relevant payee.

7.4 We reserve the right to remove any unused payee(s) from the Account without notice if the Customer has not made any Instruction to such payee(s) for a period of [13] months or more.

7.5 We reserve the right to refuse to act on an Instruction if it does not comply with these terms and conditions, our General Terms and Conditions, or the Terms and Conditions of the Account. For example, we will not ordinarily allow a transaction if it would create an overdraft, it would exceed an agreed overdraft limit, instructions are unclear or we consider that following an Instruction might be contrary to applicable law or code.

7.6 In circumstances where we refuse to carry out an Instruction, we will inform you and where possible, tell the Customer our reasons for doing so. There may be circumstances beyond our control or legal reasons that prevent us from disclosing the reason why we have refused to act on an Instruction.

7.7 We may, from time to time, apply limits to Instructions, in relation to amounts individually, in aggregate or on other criteria. Limits will come into effect immediately after we apply them. We will notify the Customer as soon as practicable.

7.8 Should we fail to execute any Instruction under the Service, or there is an undue delay of three (3) Business Days or more where there are no grounds for suspicion of the circumstances detailed in Clause 4.7 above, we will, without undue delay, refund the amount of the non-executed or defective Instruction. In addition to this, we will restore

the debited Account to the state in which it would have been had the defective Instruction not taken place.

7.9 We will not be liable for any failure to provide the Service (in whole or in part) for any cause that is beyond our reasonable control or that is unavoidable. This includes any suspension of the Service resulting from maintenance and upgrades to our systems.

7.10 We will not be liable for any delay in carrying out the Instructions while monitoring the Account and / or while fraud prevention checks are taking place.

7.11 We will not be responsible for any loss or damage that the Customer suffers if we decide not to carry out an Instruction.

7.12 If incorrect information is provided to us or there is an error in the Instruction, we will make all reasonable efforts to reverse or delete such Instruction but the Customer will be liable for any losses that result from such Instruction.

8. Timing of Instruction

8.1 Instructions received through the Service for your Account(s) before the Cut-Off Time on any Business Day will normally be processed on the same Business Day.

8.2 The Cut-Off Times applicable to Instructions placed using the Services are as follows:

Instruction Type	**Cut off time (UK Time Monday to Friday excluding UK public/bank holidays)**
Domestic Payment	4:30pm
Overseas Payment	3.30pm
Express Payment	3.30pm
Transfer to another BEAUK account	5.30pm
Carrying out a currency exchange	4.30pm
Establishing a fixed time deposit	5:30pm

8.3 Instructions received after the Cut-Off Time on a Business Day or any time on a non-Business Day will normally be processed on the next Business Day.

8.4 The User will receive notification via the Service or via other means if any Instruction is rejected.

9. Your Responsibilities and Liabilities

9.1 The Customer must inform us promptly of the following:

(a) the information, as required by us from time to time, including but not limited to the name and passport number of any person who becomes an additional or a replacement for an Administrator, and

(b) the removal of any Administrator's authority.

Until we are notified of this, Instructions from the relevant Administrator will be treated as valid and binding on the Customer, and the Customer will be liable for the outcome of any such Instruction.

9.2 The Administrator must inform us promptly of the following:

(a) the information, as required by us from time to time, including but not limited to the name and passport number of any person who become an additional User and its relevant authority level;

(b) the removal of any User;

(c) the change in any User's authority; and

(d) the change in Limit and Approval Arrangement.

Until we are notified of this, Instructions from the relevant User within their current granted authority will be treated as valid and binding on the Customer, and the Customer will be liable for the outcome of any such Instruction.

9.3 The Customer warrants to exercise due care and good internal control within the Customer's operations from time to time and to use the best efforts to implement segregation of duties and control among personnel in relation to the use of the Service.

9.4 The Administrator must contact us without delay by telephoning us on 020 7208 7090 during business hours, Monday to Friday 9:30am to 4:00pm, if User Security Details have been stolen or are liable to misuse or the User suspect that there has been unauthorised access to the Account via the Service. We may ask the Administrator to confirm this in writing within 7 days.

9.5 In accordance with Clause 4.13, the Customer will be liable for the full amount of all activities resulting from any use of the Service, save where the circumstances in Clause 4.12 have occurred.

9.6 In the event that there is a dispute regarding an Instruction, the Customer agrees that we may inform the police and our insurers and the Customer will be required to co-operate with us and the police during any investigations. The Customer agrees that we will provide the police and/or our insurers with any information that we or they consider relevant to the investigation.

9.7 The User will be able to access the Service provided that the equipment used is compatible with our requirements. For full details of these requirements, please see our Frequently Asked Questions ("FAQs") that is posted on the Website. We reserve the right to change the minimum specification that the User requires to access the Service at any time. The User should ensure that the computer equipment remains in good working order and that the User takes all reasonable steps to ensure that the computer is virus free.

10. Our Responsibilities and Liabilities

10.1 To the extent permitted by law, the Service are provided "as is" and without warranty and all warranties, terms and other conditions not expressly set out in these terms and conditions (whether implied by law, custom, statute or otherwise and including without limitation any term as to satisfactory quality or fitness for purpose) are excluded.

10.2 We do not guarantee that the Service will be available on a continuous and uninterrupted basis. We take no responsibility for, and will not be liable for, the Service (whether in whole or in part) being unavailable due to technical or other issues beyond our control or unavoidable events. This includes, in particular, any suspension of the Service resulting from maintenance and upgrades to our systems or the systems of any party used to provide the Service, outage of any phone network or in the case of mobile networks, where you are not in an area of mobile coverage.

10.3 The User hereby acknowledge and agree that we shall not be liable for any damage or loss to your software, terminal, equipment (including but not limited to mobile phones and other mobile devices) or related facilities or any loss or corruption of Customer data in connection with the operation of the Service.

10.4 We may provide hyperlinks to other websites which are not under our control. We do not investigate, verify, monitor or endorse the content, accuracy, or any opinions expressed within these websites. These links are provided for User convenience only.

10.5 The mobile service provider may not allow the User to receive OTP via SMS, if going abroad or using an overseas mobile service network. In addition, service charges may be levied by the service provider for receiving the OTP. We shall not be liable for any such charges levied by the service provider or any other party.

10.6 The delivery of the OTP via SMS may be subject to delayed transmission due to the traffic over the network of your mobile service provider. We shall not be liable for any loss or damages arising out of any interruption or delays due to any failure of the mobile service network.

10.7 We may, from time to time, suspend access to the Service so that we can carry out maintenance or update the service. We will display on our website in advance the times when the Service is likely to be unavailable, although this may not always be possible.

10.8 We reserve the right to modify and/or update Website or the BEA UK App at any time.

10.9 We are not liable for the consequences arising out of inaccurate or incorrect information supplied by the Customer or any User.

11. Fees

11.1 We do not charge User for using the Service or the BEA UK App. However, User should be aware that mobile network operator may charge for the data service, including but not limited to the charges for using the General Packet Radio Service ("GPRS"), Short Message Service ("SMS"), and any roaming charges in connection with the use and operation of the Service/ BEA UK App. These charges may vary if User access the Service/ BEA UK App when abroad. Notwithstanding anything herein to the contrary, User confirm and warrant that we shall not be involved in or in any way liable for any dispute between them and their mobile network operator or between a mobile network operator and any third party.

11.2 Fees will apply for certain services we offer through the Service. These will be detailed in the General Terms and Conditions and/or and Product Terms and Conditions. Where a fee relates to a particular type of transaction, the User will be notified of any applicable fee before the User completes a transaction. Once the User proceeds with a transaction, the Customer authorises us to debit the Account with the relevant fee(s). Please refer to our Bank Charges Leaflet for our current fees or contact us on 0808 180 3838 for details.

12. Contacting Each Other via the Service

12.1 The User may send us and we may send secure email messages to the User via the "Messages" function which is a secure function within the Service. If the User sends us a message we will aim to respond to the User within two Business Days. We shall only be deemed to have received the messages when the message is actually received by us.

12.2 The User must not send to us via the "Messages" function those messages:
which are urgent and require immediate action;
(a) which are requests of a transactional nature, e.g. relating to the creation of a new fixed deposit, making a transfer or payment etc;
(b) which report the loss or theft of cheques;
(c) which are on behalf of any third party or in relation to our dealings with any third party;
(d) which are offensive or otherwise inappropriate.

12.3 We may send messages concerning the Account(s), products or services the Customer holds with us / we offer, including matters related to the Service through the "Messages" function.

12.4 All rights in information submitted to us through the Service and Website shall be deemed to be and shall remain our property.

13. Terminating or Suspending the Service/ BEA UK App

13.1 There is no minimum contract period and the User is free to cancel the Service at any time. Please refer to the [UK Corporate Cyberbanking FAQs] for further details on how to cancel the respective Service.

13.2 If the UK Corporate Cyberbanking Services are cancelled, any access via the BEA UK App will also be cancelled automatically.

13.3 The closure of an Account by the User or us will result in the termination of the Service (including the use of the i-Toker Service) for that Account. All outstanding, pending and scheduled Instructions submitted via the Service for this Account will be automatically cancelled upon closure of the Account.

13.4 The Customer or the Administrator can notify us at any time if the Customer no longer wishes to use the Service by writing to us or in person at one of our branches. If the Customer or Administrator notifies us by other means, we may ask you to confirm this in writing.

13.5 You acknowledge that it is your User responsibility to delete the BEA UK App from the device use to access the BEA UK App if your User change or dispose of the device or you cancel or end your contract with us under clause 13.4.

13.6 Please note, deleting the BEA UK App will not end the Agreement with us for the Service.

13.7 If all Accounts are closed but the BEA UK App is retained, the Service will no longer be available to the User, and the i-Token Service shall cease to function, but generic information may be accessible in relation to other services and products that may be available or displayed via the BEA UK App.

13.8 We may terminate all or any part of the Service at any time by giving the Customer not less than two months' notice.

13.9 We may terminate the Service immediately if there is any change of law which prohibits or renders illegal the maintenance or operation of the Service or any parts thereof.

13.10 We may suspend all or any part of the Service in certain circumstances, including but not limited to the following:

(a) to protect the security of the Service or our systems;

(b) we have reason to believe that there may have been (or there is likely to be) unauthorised or fraudulent use of the Service;

(c) we have reason to believe that there has been a breach of these terms and conditions; or

(d) we are required to do so by any law or other regulatory requirement affecting us.

13.11 We may suspend User access to the Service if the User does not log in for more than 12 months, be it through the BEA UK App or otherwise.

13.12 We may terminate or suspend the User access to the Account via the Service with immediate effect in accordance with section 17.5 of our General Terms and Conditions.

13.13 On termination the Customer will immediately ensure that no Users attempt to access or use the Service.

13.14 If we terminate or suspend the use of the Service, where possible we will give you prior notice, by telephone or letter, unless we have good reason for doing so, e.g. we consider the Account(s) has been or is likely to be misused. If we are unable to contact the User, Customer or Administrator beforehand, we will notify and give reasons afterwards.

13.15 We reserve the right to withdraw the BEA UK App at any time. If we decide to do so, we will let you know in the manner set out in our General Terms and Conditions section 21(Changes to the Agreement).

14. Limitations

14.1 The information contained on the Website is provided by us. Whilst we use reasonable endeavours to keep the information up to date and correct, we make no representations or warranties of any kind, expressed or implied, about (and accept no liability for) the completeness, accuracy, timeliness, reliability, suitability or availability of any information contained on the Website. We reserve the right to modify the content and/or the design of the Website at any time without notice.

14.2 Any reliance which the Customer place on such information is therefore strictly at the Customer's own risk.

14.3 We have used reasonable endeavours to ensure, as far as possible, that emails and Instructions sent via the internet are not subject to interference and remain secure and confidential. We cannot, however, guarantee the absolute security of emails and Instructions sent via the Internet. By submitting Instructions and making use of the Service, the Customer is deemed to acknowledge and accept this.

14.4 Save where the law requires, we will not be liable for any loss or liability resulting from any failure, act or omission by the Customer's computer or software, or any Internet

browser provider, Internet access provider, online service provider or by any agent or subcontractor for any of the above.

14.5 Nothing on this website should be considered as providing financial advice. It is recommended that the Customer consults an independent financial advisor.

14.6 We shall not be liable for any indirect, special or incidental or consequential damages loss (whether foreseeable by the Bank or not) arising from or in connection with the provision of the Service and we shall not be liable for any damage to the Customer's terminals or related facilities or any loss or corruption of the Customer's data in connection with the operation of the Service.

14.7 Subject to the provisions herein, our liability (if any) to the Customer in relation to the provision of the Service shall be limited to the amount of the relevant transaction.

14.8 Nothing shall exclude or limit our liability for:

- Death or personal injury caused by negligence;
- Fraud or fraudulent misrepresentation; or
- Any liability that cannot be excluded or limited by law.

15. General

15.1 We reserve the right to amend or terminate these terms and conditions. Please refer to section 21 (Changes to the Agreement) in our General Terms and Conditions. We will give the Customer two months prior notice in writing of any changes which are material.

15.2 A copy of these terms and conditions may be obtained by the Customer from our Website or by calling our Cyberbanking Helpdesk on 020 7208 7090.

15.3 We may record or monitor telephone calls in order to establish the existence of facts or compliance with certain regulatory or self regulatory practices, ascertain or demonstrate standard to be achieved by our staff, prevent or detect crime, and other reasons permitted by law.

15.4 These terms and conditions are governed by the laws of England and Wales.

15.5 These terms and conditions and any information or notifications given under it are only available in English.

16. Use of Cookies

16.1 By using the Service, the User agrees that we may store and access cookies on the device used to access the Service which are needed to use login via the BEA UK App. For details on the cookies that we use, please refer to our Cookies Information which can be found on our Website.