BEA東亞銀行

UK Corporate Cyberbanking Service Terms and Conditions

1. Introduction

This document sets out the terms and conditions that apply to the use of the UK Corporate Cyberbanking Service (the "**Service**").

As well as these terms and conditions, you should also read:

- our Privacy Notice;
- our Cookie Information;
- our General Terms and Conditions; and
- our Products Terms and Conditions.

You can find these on our Website or in branch.

You may also find it helpful to review our UK Corporate Cyberbanking FAQs ("**FAQs**") which you can also find on our Website.

In the event of any inconsistency between these terms and conditions and our General Terms and Conditions and/or the Products Terms and Conditions in relation to the use of the Service, the terms and conditions set out in this document will apply. 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 appointed by the Customer to act on its behalf (including by appointing any Approvers) and to be responsible for managing and controlling how the Customer uses the Service from time to time;

2.3 "**Approval Arrangement**" means the number of Approvers (one or more) that must approve a transaction in order for it to be submitted (as set by the Bank from time to time);

2.4 "**Approver**" means a person appointed 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 UK bank holidays) 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. These are as defined in clause 8 of these terms and conditions and vary from the cut-off times specified in the General Terms and Conditions;

2.12 "**Cyberbanking Number**" means the unique identifier allowing a User to access and use the Service;
2.13 "**Enquirer**" means a person appointed by an Administrator who can make enquiries about an Account and any other information available via the Service for and on behalf of the Customer;
2.14 "**Inputter**" means a person appointed 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's 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 a 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's 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 Breach**" means any unauthorised use of the User's Security Details or unauthorised access to the Account via the Service, as further described in clause 4.17 of these terms and conditions;
2.23 "**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;
2.24 "**Security Code**" means a one-time numerical code generated through i-Token Service to login and/or confirm transactions performed via the Service;
2.25 "**User**" means an Administrator, Enquirer, Inputter or Approver; and
2.26 "**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. Purpose of the Service and application of these terms

3.1 The Service enables the Customer to carry out certain banking functions in the Accounts that you have with us via the internet;
3.2 All Accounts and payee templates that you have registered will be accessible via the Service;
3.3 By using the Service, you accept these terms and conditions. You are strongly advised to read the terms and conditions before using the Service;
3.4 The Customer is only permitted to use the Service in accordance with these terms and conditions;
3.5 In addition to these terms we may provide you with instructions at any time (using any method of communication agreed between us and the Customer) about how the Service should be accessed; and

3.6 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 FAQ 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.

4. Security

Checking Users

4.1 The Customer should ensure it regularly assesses the competency, honesty, integrity and suitability of all Users. If you have concerns about a User, you must not allow them to access the Service and should remove their access rights.

4.2 The Customer must tell each User to observe and comply with reasonable security precautions relating to online banking services. Reasonable security precautions would include:

- Keeping vigilant at all times and avoiding clicking on embedded hyperlinks in any communication that appears to have been sent by us that the User has reason to believe may be suspicious;
- Never disclosing login information needed to use the Service to a third party;
- Regularly ensuring your information held by 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.

Security tips and FAQs are available when logging in to the Service and on our Website.

4.3 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.

Security Details

4.4 Where relevant, the Administrator shall collect the Security Details for the Service for each relevant User 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. When the Administrator has these, the Administrator shall pass the relevant Security Details to the relevant Users.

4.5 The Customer will require that each Administrator and each other User keep the Security Details given to them secure.

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

4.7 If the User did not enrol for i-Token Service, the User will continue to receive an OTP that must be used when accessing the Service. The OTP is sent to the User's registered mobile phone number as an additional level security. Without using i-Token, you may not be able to access all Services. For more information, please refer to Q12.3 in our UK Corporate Cyberbanking FAQ for details.

4.8 If the User chooses to use fingerprint or any other means of biometric identification to generate the Security code, then the Customer/User agrees that these forms of authentication can be used to log in to and confirm certain transactions in the Services. Users 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.

4.9 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 Service in order to continue to use the Service.

Security Breaches

4.10 The Customer will check its Account balances and transactions regularly. If the Customer suspects or has become aware of 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.

4.11 A User must contact us as soon as possible by telephoning us on 020 7208 7090 between 9:00am to 5:00pm on Business Days if a User's Security Details have been stolen or could be misused by someone else, or a User suspects that there has been unauthorised access to the Account via the Service. If a User fails to do so, and in any event within 13 months after the date on which this occurred, you may not be entitled to have any error corrected, payment amount refunded or to be compensated for any loss suffered. We may ask the Administrator to confirm the theft/misuse of your details in writing within 7 days.

4.12 In the event of suspected or actual fraud or a security threat, we will contact the affected User via a means of contact which we consider secure, which may be the affected User's registered phone number (provided it is different to the phone number to which your i-Token is registered) and/or e-mail address, providing the individual with details of the activity itself and measures we are taking to protect the Account.

4.13 We can refuse, block and/or delay any Instruction if we think that:

- the security of the Service, your Account, or a payment, has been compromised;
- someone else is making the Instruction and you didn't agree to this; or
- in the event that the Account offers an overdraft facility, there is a significantly increased risk that the Customer would enter the overdraft but may be unable to fulfil its liability to repay the overdraft.

4.14 If we think any of the circumstances in Clause 4.13 may have happened, if we are allowed to, we will try to tell the User before we refuse, block and/or delay the Instruction, and tell the User how to solve the problem. We might not always be able to do this, and if we can't tell the User before we take the action, we will tell them as soon as we can after it (again, provided we are allowed to),

4.15 Once an issue is solved and/or the User has been provided with new Security Details, we will make the Service available to you again as soon as possible.

4.16 For more information on all types of fraud and how to prevent becoming a victim, please visit the government website at www.moneyhelper.org.uk.

Liability for Security Breaches

4.17 The table below illustrates scenarios for a Security Breach where we or you may be liable for the whole or a portion of the losses from your Account.

Security Breaches for which we won't refund you	
Situation	**Outcome**
A User or Customer authorised the transaction	We will not refund you. (You will be responsible for the full amount of the transaction.)
A User or Customer agreed to provide Security Details to another person	
A User or Customer failed to use Security Details in accordance with these terms and conditions	
A User or Customer failed to notify us in accordance with clause 4.11 of these terms and conditions and without undue delay on becoming aware of the loss, theft or misappropriation of Security Details	
The User or Customer has acted fraudulently	

Security Breaches for which we will refund you	
Situation	**Outcome**
The loss, theft or misappropriation of the Security Details was not detectable prior to the payment for reasons other than the User or Customer acting fraudulently	We will refund you in full.
The loss occurs before the Security Details have been received or set up by the User or Customer	
The loss occurs after the User or Customer has notified us that Security Details have been lost, stolen or used without authorisation	
We have failed to tell the User or the Customer how to notify us of any loss, theft or unauthorised use of Security Details	
We do not apply procedures that we are legally required to use to check a payment has been authorised by the User or the Customer	
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	
In any situations that are not covered by Security Breaches for which we won't refund you (e.g. losses that occur before the User notifies us of any loss, theft or unauthorised use of Security Details, but the User has not acted fraudulently or been negligent with Security Details)	We will refund you, but we may not refund the first £35 of the transactions. (You will be responsible for the first £35 of any losses you suffered.)

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 wishes 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. Please refer to the i-Token activation demo for details, which you can find on our Website. 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 wishes to enrol i-Token on a different device, the User should follow any instructions the User may get in the BEA UK App and on the Website about how to do this.

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 afterwards without internet access.

6. Support for the BEA UK App

6.1 In order to use the BEA UK App a User must have a compatible device running the most up-to-date version of the operating system for that device.

6.2 A User may not be able to use the BEA UK App until they have downloaded the latest version of the BEA UK App and accepted any new terms.

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

6.4 We may stop supporting the BEA UK App on a User device or on the version of the operating system running on the User device. If that 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 has updated the operating system on that device, as applicable.

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

7. Acting on the Customer's Instructions

Appointing Users

7.1 Customers must 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. An Administrator shall manage and control the access and use of the Service including without limitation the appointment of Users (determining which individuals have access to which functionality within the Service, including the authorisation of Instructions to the Bank) and the distribution of PINs to Users as set out in these terms and conditions. The Instructions given by an Administrator or an Approver will be binding on the Customer.

7.2 The Customer must inform us promptly of the following:

- any information we may request about any person who is added or replaced as an Administrator (for example, their name and passport number), and
- the removal of any Administrator's authority.

7.3 If a Customer has removed an Administrator's authority but the Customer has not told us this, the Instructions from the relevant Administrator will still be treated as valid and binding on the Customer, and the Customer will be liable for the outcome of any such Instruction.

7.4 The Administrator must inform us promptly of the following:

- any information we may request about any person who will become an additional User and the User's relevant authority level;
- the removal of any User;
- the change in any User's authority; and
- the change in Limit and Approval Arrangement.

7.5 If a Customer has removed or changed a User's authority but the Customer has not told us this, the Instructions from the relevant User that are within their previous

authority will still be treated as valid and binding on the Customer, and the Customer will be liable for the outcome of any such Instruction.

7.6 The Customer agrees that it will attempt to segregate duties and control between appointed Users in relation to the use of the Service to avoid conflicts of interest and/or Security Breaches.

Submitting Transaction Instructions

7.7 In order for us to act on an 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.

7.8 We will act on Instructions submitted by a valid User via the Service. Provided the correct Security Details are used, we may not carry out further checks on who is submitting the Instruction or question the details of the transaction, so Users should protect their Security Details as much as possible.

7.9 Where an Instruction relates to a payment or a transfer, please refer to our General Terms and Conditions to understand how it will be effected.

7.10 We may, from time to time, apply Limits to Instructions. Limits will come into effect immediately after we apply them. We will notify the Customer as soon as practicable.

7.11 Once we have received an Instruction from a valid User, they won't normally be able to cancel or change that Instruction. We will keep a record of all Instructions we receive and how these are handled by us, and may use this to prove what happens at a later date.

7.12 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.

Payees for Instructions

7.13 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.

7.14 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.

Refusing Instructions

7.15 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, Instruction is unclear, we suspect the Instruction may be fraudulent or we consider that following an Instruction might be contrary to applicable law or code.

7.16 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.

Your liability for incorrect Instructions

7.17 If a User provides us with incorrect information 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.

Our liability for Instructions

7.18 If
(a) we debit money from your Account but it doesn't actually reach the person you asked to be paid;
(b) there is a delay of three (3) Business Days or more in the time that money that we debited from your Account should have reached the person you asked to be paid and there is no good reason for this delay; or
(c) we send the wrong amount to someone or send an amount to the wrong account,
we will, as soon as possible, refund your Account with the amount of this transaction. In addition, we will compensate you for any fees or similar that we charged because of such payment.

7.19 We will not be liable for any failure to provide the Services (in whole or in part) when we need to perform repairs, maintenance, or updates to our systems, in the event of a failure of our systems which is outside of our reasonable control or for any other cause that is beyond our control (for example, war, explosion, earthquake, etc.).

7.20 We will not refund you for any costs you incur (for example, fees or interest payments) which happen because we delayed a User's Instruction in order to check that the Instruction had been approved by such User or you and/or carry out financial crime prevention checks (provided the length of the delay is reasonable for our checks, etc.).

7.21 Additionally, if we decide not to go ahead with an Instruction because we have legitimate concerns about it not being from you or that it would break the law (or similar), we will not refund you for any costs you incur (for example, fees or interest payments) which happen because of this.

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. Our Responsibilities and Liabilities

9.1 These terms and conditions together with the documents set out in clause 1 above contain all of the provisions relating to the offer of the Services and no other terms and conditions (whether arising from law, custom, statute or otherwise and including without limitation any term as to satisfactory quality or fitness for purpose) are treated as applying.

9.2 We will make every effort to ensure that the Service will be available on a continuous and uninterrupted basis. The Service (whether in whole or in part) may be unavailable due to technical or other issues beyond our reasonable control or from 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. Where possible we will give you advance notice of any interruption to the Service and will advise you on alternatives for accessing our services during this period.

9.3 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's convenience only.

9.4 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.

9.5 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.

9.6 We may, from time to time, suspend access to the Service so that we can carry out maintenance or update the service. We will use all reasonable endeavours to let you know in advance the times when the Services are likely to be unavailable and for how long, although this may not always be possible. Please refer to the 'Maintenance schedule' on our Website for details. We will also advise you how else you can access your accounts and other products during this time.

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

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

10. Fees

10.1 We do not charge Users for using the Service or the BEA UK App. However, Users should be aware that mobile network operators 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 Users access the Service/ BEA UK App when abroad.

10.2 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.

11. Contacting Each Other via the Service

11.1 Users may send to us and we may send to Users, secure email messages 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.

11.2 The User must not send to us via the 'Messages' function those messages:

- which are urgent and require immediate action (these should be given by telephoning us on 020 7208 7090 between 9:00am to 5:00pm on Business Days);
- which are requests of a transactional nature, e.g. relating to the creation of a new fixed deposit, making a transfer or payment etc. (these should be done through the Services/submitting Instructions); or
- which report the loss or theft of cheques or any Security Breaches (these should be given by phone as detailed under clause 4.11 above).

11.3 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. However, we will not contact you in relation to an account other than your Account nor will we discuss with you our dealings with an account that is not owned by you.

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

12. Terminating or Suspending the Service/ BEA UK App

Customer terminating the Service

12.1 There is no minimum contract period, the Customer or an 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 the Customer to confirm this in writing.

12.2 If the Services are cancelled, any access via the BEA UK App will also be cancelled automatically for all Users.

12.3 The closure of an Account will result in the termination of the Service (including the use of the i-Token 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.

Users access

12.4 There is no minimum contract period and the User is free to cancel their access to the Service at any time. Please refer to the UK Corporate Cyberbanking FAQs for further details on how to cancel the respective Service for a User or for the Customer as a whole.

12.5 It is a User's responsibility to delete the BEA UK App from a device used to access the BEA UK App if the User changes or disposes of the device or you cancel or end your contract with us.

12.6 Please note, deleting the BEA UK App on its own will not end the User's authority (under this Service or more generally in respect of the Accounts) or terminate the Service, the Customer must amend the User's authority or terminate the Service itself to effect this.

12.7 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.

Where we may terminate or suspend the Service

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

12.9 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.

12.10 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. We may close your Account immediately if any of the following happen:

- You put us in a position where we might break a law, regulation, code, court order or other duty or requirement;
- You have given us false or misleading information;
- You use or try to use your Account illegally or for criminal activity, including receiving proceeds of crime into your Account – or you let someone else do this;
- You commit (or attempt) fraud against us or someone else;
- You behave in a threatening or abusive manner against our staff;
- You have seriously or persistently broken these terms or any other relevant terms relating to the Service, such our General Terms and Conditions; or
- You have moved to a country that we consider sensitive for the purposes of trading.

12.11 On termination of the Service as a whole or for an individual User, the Customer will immediately ensure that no Users/the affected User does not attempt to access or use the Service.

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

- to protect the security of the Service or our systems;
- we have reason to believe that there may have been (or there is likely to be) unauthorised or fraudulent use of the Service;
- we have reason to believe that there has been a breach of these terms and conditions; or
- we are required to do so by any law or other regulatory requirement affecting us.

12.13 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.

12.14 If we terminate or suspend the use of the Service, where possible and to the extent permitted by law we will give you prior notice, by telephone or letter, unless we have good reason for not 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.

12.15 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).

13. Limitations

13.1 The information contained on the Website is provided by us and we shall use best endeavours to keep such information up to date and correct. We may modify the content and/or the design of the Website at any time without notice. Nothing in this clause 13.1 shall impact the information in relation to your Account balance or payment transactions as accessed via the Services.

13.2 Any reliance which the Customer places on such information is therefore strictly at the Customer's own risk. This means that if you suffer any loss as a result of acting, or choosing not to act, on the basis of such information, we will not be required to compensate you.

13.3 We have tried, as far as possible, to make sure 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.

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

13.5 We shall only be liable for any losses which are the natural results of a breach in the usual course of things. If losses arise from a special circumstance of the incident, we will not be liable for these (whether we could foresee the loss or not) arising from or in connection with the provision of the Service – this means we will not normally be liable for matters such as:

- loss of business;
- loss of goodwill;
- loss of opportunity; or
- loss of profit.

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 (except where it can be proven we were directly responsible for the loss or corruption).

13.6 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.

13.7 Nothing shall exclude or limit our liability for:

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

14. General

14.1 We reserve the right to amend or terminate these terms and conditions. The process for amending our terms and conditions is set out in 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 material changes.

14.2 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.

14.3 If you are not happy with any part of these Service or you think we have made a mistake, please let us know. Please refer to section 24 (Complaints) in our General Terms and Conditions for further details on how we will handle this and what rights you may have to contact the Financial Ombudsman Service.

14.4 You may contact us about the Services using the methods and details referred to in Section 2 (Contacting each other) in our General Terms and Conditions. We may record or monitor telephone calls in order to ensure security for our customers and our staff and to help maintain service quality.

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

14.6 These terms and conditions and any information or notifications given under it are only available in English. If you have difficulty understanding anything – please tell us and we will do our best to help you.

15. Use of Cookies

15.1 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.

Oct 2024