ធនាគារ ស៊ីស៊ីយូ ខមមែសល ម៊ែង ម.ក
CCU COMMERCIAL BANK Plc.

CCU Mobile Banking

Terms and Conditions

05 September 2023

Version 1.0

CONTENTS

MOBILE BANKING TERMS AND CONDITIONS

These terms and conditions governing all types of Mobile Banking (Mobile Banking Terms and Conditions) are provided by CCU COMMERCIAL BANK PLC. (Bank). Mobile Banking allows customers to access to view accounts and some of our mobile banking services are made available in CCU Mobile from time to time in a format that is easier to view and to take effective transactions on customer's smartphone. As a user of Mobile Banking, it is very important for customers to read the Specific Terms and Conditions carefully. By registering for and using Mobile Banking's customers agree to be bound by the Specific Terms and Conditions. By pressing "**Accept**" customer the confirms that the customer is acting on customer behalf and not on behalf of a third person, and that the customer has read, understood, acknowledged, accepted, and given the customer express consent to the Specific Terms and Conditions.

For more detailed information about Mobile Banking please refer to the FAQs available at any CCU's branch and on our official website www.ccubank.com.kh.

1. DEFINITIONS

The following words/expressions shall have the meanings as respectively set out below unless the context requires otherwise:

1.1. **CCU Mobile Banking** means an application for a smartphone that can be downloaded by the Customer from the following application stores App Store or Google Play.

1.2. **CCU Payment** means a mobile-based payment facility enabling CCU Mobile users to make payments or purchases from their CCU Accounts or linked Visa/Mastercard at stores or online merchants by scanning a compatible Quick Response (QR) code.

1.3. **Account** means and includes CCU's Savings Account, Current Account, and Fixed Deposit Account in both KHR and USD currencies as may be created from time to time at CCU branch or via Mobile Banking.

1.4. **Biometric Identifier** includes a fingerprint, facial data, and any other means by which a mobile device manufacturer allows a user to authenticate their identity for the purposes of unlocking their mobile device and accessing specific applications including Mobile Banking.

1.5. **Card** means and includes CCU's debit/credit card with varied schemes such as VISA/ Mastercard/ UPI in the form of either virtual or plastic one.

1.6. **CIF** means a unique customer identification number used in the Bank's system that the customer receives during customer's first account registration with CCU.

1.7. **Content** means and includes any information, images, links, sounds, graphics, video, software, or other materials, including quotes, news, and research data, made available through Mobile Banking.

1.8. **Customer** Includes CCU account holder and non-CCU account holder that acquire one-off services from CCU Bank. All customers are subject to different forms of due diligence.

1.9. **Fixed Deposit Certificate** means an informational electronic document of customer Fixed Deposit Account details opened via Mobile Banking or at CCU branch.

1.10. **Notification** means the SMS or in-app push notifications sent to you on different occasions related to banking transactions or general alerts sent by CCU.

1.11. **Username** means a unique string of the customer's identity used to log in to CCU Mobile.

1.12. **Password** means secret data, typically a string of characters, number, and special characters, it is used to confirm a customer's identity to log in and access CCU Mobile.

1.13. **PIN or PIN Code** means the six (6) digit number used to log in to CCU Mobile and to confirm any transaction.

1.14. **OTP** means a one-time-password, it is a unique six (6) digit number sent to the customer's primary phone number and used to confirm any transaction.

1.15. **Self-Register** means a mobile banking service that allows customers who already have the CCU Account but ever registered the the mobile banking service before and they wish to use mobile banking, and they can perform mobile banking registration by themselves.

1.16. **Transaction** means any financial record or operation made or performed, processed or effected by you or any person purporting to be you, or any person purportedly acting on your behalf, with or without your consent,

including any payment or fund transfer to/from your account; any other banking transaction that may be made available through CCU from time to time (including making bill payments); and any banking transaction carried out through any CCU branch.

1.17. **Transfer** means fund transfer whereby CCU becomes a paying or receiving bank on behalf of you to take effect any payment order made to/from you. Transfers include both local transfer and international transfers, for example, a transfer from you to another beneficiary within CCU or to a beneficiary in other financial institutions such as banks or microfinance.

1.18. **Personal Information** means the personal information provided by you to CCU, including but not limited to name, national identity number (NID), date of birth, phone number, email, and address.

1.19. **Mobile Operator** means the mobile phone service provider who provides the mobile network.

1.20. **Jailbroken or Rooted** means that a smartphone or other mobile device is modified to remove restrictions imposed by the manufacturer or operator to allow the installation of unauthorized software.

1.21. **Security Credential** refers to the customer's CIF, Password, PIN, OTP and other information that the customer can use to access the Mobile Banking service.

1.22. **We, us, our, ours** refer to CCU Commercial Bank Plc.

1.23. **You, your, yours** refer to an account holder and mobile banking user.

2. SERVICE DESCRIPTION

2.1. Key features of Mobile Banking:

a. Accounts
- View account information.
- View account balance.
- View account statements.
- Open a new account savings or current account.

b. Cards
- View card information.
- Set limitation of amount and transaction for the card.
- Activate new card.
- Bock/Unblock/Change PIN card.
- Physical card issuance.

c. Fund Transfer
- Transfers to own CCU Accounts.
- Transfer to other CCU Accounts.

d. Other services
- Locator of CCU ATM, Branch, and Digital Branch.
- View our contact information.
- View CCU announcements.

3. USER ELIGIBILITY

3.1. The CUU account holder.

3.2. The eligible smartphone/device.

3.3. The device OS iOS or Android

3.4. The valid and active mobile phone number.

3.5. The valid and active CCU debit card number.

3.6. Mobile Banking on Customer's devices using a valid phone number registered with CCU.

3.7. Customer acknowledges that CCU reserves the right to reject customer requests for Mobile Banking activation without assigning any reason during the activation process.

4. FEES AND CHARGES

4.1 Mobile Banking is free to use. However, fees and charges may apply when the customer makes certain transactions or uses specific products or services available in Mobile Banking in accordance with the specific Terms and Conditions. The customer authorizes CCU to debit from the customer account these fees and other applicable charges as described in the respective specific Terms and Conditions. CCU may introduce additional fees and charges for customer use of Mobile Banking from time to time, and fees and other charges may also be changed by CCU from time to time. Details of CCU's current fees and charges are available at any branch or at CCU's website www.ccubank.com.kh. Before making any transaction, the customer agrees to check the current fees and charges, and Customer agree to accept these fees and charges by making a transaction.

4.2 Customers may incur charges from the customer's mobile service provider for downloading, updating, and using CCU Mobile. Any such charges are the customer's sole responsibility and any matters regarding these charges should be raised with the customer mobile operator. Customers should contact the mobile operator for more information on their fees and charges.

5. LIMITATION OF SERVICES

5.1. Transaction Limits

As part of constant risk mitigation measures, CCU reserves the right to set and change limitations on the transaction amount, number of transactions, condition, as well as transfer destinations, and other matters at any time without giving prior notice.

5.2. Connectivity

5.2.1. Bank shall not be liable to a customer for any incompleteness, unavailability, failure, interruption, suspension, or delay in Mobile Banking (including the transmission of any alerts or notifications or in receipt or execution of any instructions) due to any factors not under bank's reasonable control.

5.3. System Maintenance

5.3.1. Bank may add or disable any features or suspend the operation of Mobile Banking or any of its services at any time. If, in CCU's opinion, any threat is posed to any Mobile Banking related system or part of any system; or for the purposes of carrying out periodic maintenance and administration tasks.

5.3.2. Mobile Banking is a constantly evolving application that will have frequent releases in order to bring new features and improvements, as well as updated operating systems. Customers must update and use only the most up-to-date version of Mobile Banking.

5.3.3. From time to time, CCU may force its users to update Mobile Banking to the latest version for security and compatibility reasons. Customer might not be able to continue using an old version of Mobile Banking unless the Customer updates to the latest version.

6. SECURITY

6.1 GENERAL PRECAUTIONS

6.1.1. Customer shall take responsibility for and use customer's best endeavors to prevent any unauthorized use of, and access to Mobile Banking on customer's mobile and/or other device and to protect Personal Information and Security Credentials at all times. For example, the customer must:

a) Not let any other person use Customer Security Credentials to access customer account(s) or Mobile Banking on customer's mobile device.
b) Not let any other person unlock their mobile device or store their Biometric Identifier on CCU Mobile; and/or
c) Not leave mobile device unattended while remaining logged into account(s) or CCU Mobile Banking.
d) Ensure that Security Credentials to access Mobile Banking remain confidential and that the customer takes all reasonable steps to prevent them from being disclosed. For example, the customer must memorize customer Security Credentials; and not write down or save Customer Security Credentials anywhere in any form, including electronically, for example, in customer's mobile phone or device.
e) Not disclose Security Credentials to anyone (including the police, bank staff or customer loved ones).
f) Take care to ensure that no one else can see Security Credentials; and/or
g) Not install or use Mobile Banking on mobile devices that have been jailbroken or rooted.

6.1.2. Customer must lock customer mobile device or take other steps necessary to stop unauthorized use of Mobile Banking.

6.1.3. Customers must notify the Bank immediately by calling **023 900 777** upon being aware of that.
a) Mobile devices are lost or stolen.
b) PIN code has become known or may be known by another person.
c) Another person may be able to unlock the mobile device and/or store their fingerprint(s) and other Biometric Identifiers on the mobile device if the customer has fingerprint identification enabled on CCU Mobile Banking; or
d) There has been unauthorized access to customer account(s) accessible via CCU Mobile Banking.
e) Customer notices that Mobile Banking is requesting the customer to re-activate the application (which may indicate that Mobile Banking is being activated with Customer Security Credentials on another device).

6.1.4. Customer must install only approved applications on Customer mobile device and the customer will not jailbreak or root customer mobile device.

6.1.5. Customer must promptly update, and keep updated, the operating system and security software for customer mobile device when released by customer mobile device manufacturer or mobile device operating system provider.

6.1.6. Customer must not allow any other person to store their Biometric Identifier on the customer's mobile device.

6.1.7. Before the customer sells or permanently gives the customer mobile device to any person, the customer must delete the Mobile Banking and all customer Biometric Identifiers (e.g., Touch-ID or Face-ID) registered in the device.

6.1.8. The security of Your Personal Information is important to us but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While We strive to use commercially acceptable means to protect Your Personal Information, we cannot guarantee its absolute security.

6.2. SECURITY CREDENTIALS

6.2.1. Mobile Banking and its services require the use of Security Credentials that consist of a PIN code.

6.2.2. The self-registration option enables customers to register for mobile banking without the assistance of bank employees. The customer initiates the registration process using the downloaded Mobile Banking application.

6.2.3. Customer will do self-registration using customer's mobile phone number (registered before with bank), Account Number/Customer ID/ Card number, card expiry date, and Date of Birth.

6.2.4. If the input information is valid then a one-time password (OTP) is sent to the customer's registered mobile device as part of the registration process for the purposes of verifying the customer's identity and mobile number.

6.2.5. After the customer has been authenticated, the application can request additional data, such as the customer's login name and password, and device name to complete the registration.

6.2.6. The high-level process for customer self-registration from the Mobile Banking application is as follows:
a. Customer downloads and opens the Mobile Application.
b. The customer selects Continue on the welcome screen.

c. The customer selects to register by Card number or register by CBS account number.
d. The customer inputs according to identification information:
   - If the customer selects to register by Card number, then the Mobile Application displays the following fields for the customer to enter identification information:
     - Customer's Mobile phone number.
     - Card number
     - Card expiry date
   - If the customer selects to register by CBS account number, then the Mobile Application displays the following fields for the customer to enter identification information:
     - Customer's Mobile Phone number.
     - CBS account number.
     - Customer ID card number.
     - Customer's Date of Birth.
e. The customer enters their desired device name, login, name and password/ PIN, and confirms the password/ PIN.
f. Mobile Application to send the identification input by the customer for validation:
   - If registration by card number is selected, then the Mobile Application Sever calls API to SVFE (via API Gateway/ SVIP) for validation.
   - If registration by CBS account number is selected, then Mobile Application Server calls API to CBS (via API Gateway/ SVIP) for validation.
g. Based on the successful validation result from SVFE/ CBS, the Mobile Application server generates a one-time-PIN (OTP) to the customer's mobile phone number.
h. The customer enters OTP on the Mobile Application for authentication.
i. After OTP has been validated, the customer can enable fingerprint or Face ID authentication if it is available on the device.

6.3. AUTHENTICATION & AUTHORIZATION METHODS

6.3.1. Customer as a user may choose customer preferable way to log to Mobile Banking and to confirm or to authorize banking transactions, including:
a) Use PIN or Biometrics to log into Mobile Banking.
b) Use PIN or Biometrics to confirm or authorize banking transactions. Either method will apply with its own terms and conditions including but not limited to minimum and maximum transaction limits.

6.3.2. A customer as a user with an eligible mobile device may choose to enable biometric authentication to log on to CCU Mobile Banking, transfer funds, and make payments by using a Biometric Identifier registered on Customer's mobile device. Mobile Banking does not collect or store this Biometric Identifier, and it is stored on customer's mobile device.

6.3.3. If the Customer enables or uses a Biometric Identifier to access CCU Mobile Banking, the customer must ensure that the customer Biometric Identifier is the only Biometric Identifier stored on the mobile device the customer uses to access CCU Mobile Banking. However, if another person has stored their Biometric Identifiers on the mobile device customer used to access CCU Mobile Banking, it is in breach of the Specific Terms and Conditions, and the customer acknowledges that they will be able to access customer accounts including to view and conduct certain transactions on Mobile Banking and these transactions will be treated as having been authorized by the customer and conducted with customer knowledge and consent.

6.4. JAILBREAKING AND ROOTING SMARTPHONES AND DEVICES

6.4.1. CCU strongly recommends that customers do not modify the customer operating system by jailbreaking or rooting Customer's mobile device because doing so may compromise both the performance of Mobile Banking and the security of customer banking information, including customer passwords. If a customer uses a mobile

device that has been jailbroken or rooted, the customer does so at customer's own risk. CCU Bank will not be liable for and specifically disclaims any liability for any losses or other damage the customer may incur as a result of using a jailbroken or rooted mobile device.

7. USERS ACKNOWLEDGEMENT

7.1 TRANSFERS

7.1.1. When initiating any fund transfers, the customer will be required to provide certain information about the recipient, which will vary depending on the type of transfer, and the customer agrees that CCU can store all provided information and show them in bank statements.

7.1.2. When making a transfer to a recipient with CCU Account or PSP's wallet, Mobile Banking will display the name of the recipient for the sole purpose of assisting the customer in identifying the recipient of the transfer only, and the customer agrees not to share or disclose the recipient's name to any third parties. In the event that the customer share or disclose the receipt's name to any third parties, the customer agrees that the customer will be liable for any damage or loss suffered by us (including consequential loss and regulatory fines) which results from the customer sharing or disclosure of the recipient's name and Account number to any third party in accordance with clause **[8.3.]**

7.1.3. Customers provide customer express consent that CCU can disclose customer name to any person attempting to initiate a fund transfer to the customer from their CCU Account or PSP's wallets to the customer CCU Account at that point in time that they input the customer Account number, even when the transfer may not be completed.

7.2. PAYMENT

7.2.1. For any payment / purchase transaction made via CCU Mobile, the customer agrees that we can disclose the customer's name and payment details the customer made to the vendor or merchant in order to notify and assist them in identifying the transaction.

7.2.2. We may cancel or suspend a payment at any time without notice to the recipient. Under certain circumstances, CCU Bank might not be able to cancel a payment or purchase immediately as requested by the payer. As required by applicable law or under legal arrangements, the customer will be informed through different means (including Notification) of payment failure or cancellation in different stages of reconciliation. Customers are obliged to review and acknowledge such cancellations.

7.3. QR PAYMENT

7.3.1. Customer agrees to have customer account listed and displayed when customer scans a QR code with Mobile Banking installed on the customer device. With certain validation, certain ineligible accounts are not displayed for choosing.

7.4. NOTIFICATIONS

7.4.1. SMS Notification

a) Customer agrees that, by registering for CCU Mobile, CCU may send or be requested to send an SMS to customer's mobile device.

b) CCU is not liable for any loss or damage a customer suffers as a result of any person other than the customer accessing those SMSs and their content as a result of customer negligence.

c) Customers may incur charges from Mobile Operator as a result of using Mobile Banking or SMSs. Any such charges are solely customer's responsibility.

7.4.2. Mobile Push Notification

a) Customer agrees to receive alerts or notifications for customer CCU Account for certain transactions or for marketing communications or announcements from CCU.

8. CUSTOMER OBLIGATION

8.1.1. Customer must not use Mobile Banking for any purpose other than to undertake legitimate banking enquiries or transactions on accounts customer are legally entitled to operate in accordance with the Specific Terms and Conditions and the terms and conditions applicable to the customer.

8.1.2. Customers must not use Mobile Banking for prohibited business activities.

8.1.3. Customer must not act fraudulently or maliciously in relation to Mobile Banking or software. For examples, customers must not copy, modify, adversely affect, reverse engineer, hack into, or insert malicious code into Mobile Banking or software.

8.1.4. If Customer uses photos to personalize customer accounts that can be accessed using CCU Mobile, customer warrants that:

8.1.5. The photos used by the customer does not contain content, which is offensive or illegal, or would be considered unacceptable for viewing by a person under 18 years old; and

8.1.6. Customer took the photo (or is the owner of the copyright in the photo).

8.1.7. Customer acknowledges that customer is responsible for and must take all reasonable care to ensure that information customer supplies via Mobile Banking is true, complete, accurate, and up to date.

9. LIABILITY AND INDEMNITY

9.1 CCU LIABILITY

9.1.1. CCU will not be liable for any loss arising from customer use of CCU Mobile, including loss arising from any security breach, if the customer has acted fraudulently (either alone or together with any other person), if the customer has installed applications on the customer mobile device other than those available from the Apple App Store or Google Play market, or if customer have caused or contributed to that loss, for example, by failing to comply with any of the Specific Terms and Conditions or other applicable terms and conditions. It is customer's choice to download and install CCU Mobile. To the extent permitted by law, CCU accepts no liability for any loss or consequences to the customer whatsoever that result from this decision, including in the event CCU refuses or fails to process a transaction request or delays in doing so.

9.2. LIMITATION OF CCU LIABILITY

9.2.1. To the extent permitted by law, we will not be liable to the customer for any direct or indirect costs, losses, damages, or other liabilities resulting from

a) Customer use of any service provided through Mobile Banking.

b) Customer failure to comply with the Specific Terms and Conditions.

c) Any delay or loss of access to, or use of any Mobile Operators at any time.

d) Any fault or error in the design, content, or engineering of any Mobile Operators is reasonably beyond our control.

e) Malfunction of any equipment or system, or any telecommunications link failure; or

f) Any cause or event reasonably beyond our control.

9.2.2. CCU has no authority to act for or to incur any obligation on behalf of any Mobile Operator.

9.2.3. CCU is at no time acting as an agent or partner of any Mobile Operator in providing any mobile service and no representation is made or given by CCU that any such relationship exists.

9.3. CUSTOMER LIABILITY

9.3.1. The customer acknowledges that any unauthorized reproduction by a customer of any proprietary information provided or available via Mobile Banking or any portion of it may result in legal action being taken.

9.3.2. The Customer will be liable for any loss suffered by us (including consequential loss) which results from customer fraud or negligence, or customer violation of the Specific Terms and Conditions. The customer will be liable for any loss suffered by us which results from the unauthorized access to or use of any service available in Mobile Banking and to which the customer has contributed by the customer's failure to comply with the Specific Terms and Conditions. This includes if the customer:

a) Create an unsuitable password or PIN code.

b) Fail to disable biometric authentication on Mobile Banking when the customer knows or suspects another person can unlock customer's mobile device or has stored their Biometric Identifier(s) on the customer's mobile device.

c) Fail to verify the recipient information before completing any transfer or payment which leads to either direct or indirect loss; or

d) Customer unreasonably delay notifying us of:

(i) the loss or theft of customer mobile phone or device or Security Credentials.

(ii) the actual or suspected disclosure to any other person of customer PIN code.

(iii) when the customer knows or suspects that another person may be able to unlock customer's mobile device and/or store Biometric Identifier(s) on customer's mobile device and the customer has biometric authentication enabled on CCU Mobile; or

(iv) that there has been, or customer suspect there has been unauthorized access or activity through Mobile Banking.

9.3.3. The customer will be liable for any loss suffered by the customer and us, if the customer uses a mobile device that has been jailbroken, rooted, or any unknown devices.

9.4. LIMITATION OF CUSTOMER LIABILITY

9.4.1. Customer will not be liable for any loss caused by

a) Us acting fraudulently or negligently; or

b) A fault occurs in the machines; or

c) Systems used as part of the Mobile Banking system unless such fault is obvious; or

d) The customer has been advised of such fault by a message; or

e) Notice on display and the loss occurred after such notification.

10. DISPUTES WITH MERCHANTS OR VENDORS

10.1. CCU has no liability for any purchases or payments made by Scan QR service or other payment options presented in Mobile Banking if:

a) There is any defect or deficiency in the provision of the goods or services, or.

b) Customers decide that they no longer want the goods or services.

10.2. Any such dispute is to be resolved between the customer and the merchant or vendor directly.

10.3. Customers are responsible for exercising reasonable care and being aware of the risks of paying for goods and services in advance of receiving them. Customers should consider the standing of the person or entity the customer is doing business with, including when purchasing goods or services that are not face-to-face.

10.4. Even if the Customer has a dispute with a merchant or vendor, the Customer must still pay all amounts due to us.

11. SUSPENSION OR TERMINATION OF MOBILE BANKING

11.1. Customer may cancel Mobile Banking usage at any time by notifying CCU in writing or by phone. The customer will remain responsible for any transactions made on the customer's account/s using Mobile Banking up until the time at which such cancellation becomes effective.

11.2. CCU may withdraw access at any time without giving prior notice, suspend and/ or terminate customer access to Mobile Banking or to any of its services for any reason, including (but not limited to) where CCU is of the opinion that the customer has acted in breach of the Specific Terms and Conditions.

11.3. In case a customer changes mobile device and wishes to continue using CCU Mobile, the customer must download Mobile Banking on the new mobile device and follow the registration process. The Customer may uninstall Mobile Banking from the existing devices prior to, or during, the registration process for the new devices.

12. PRIVACY TERMS

12.1. In accordance with Cambodia's regulatory requirements and CCU's internal policies, customers provide express consent and agree that:

a) As part of satisfying CCU's KYC (Know Customer Customer) requirements, Mobile Banking may collect Personal Information from customers; customers provide warranty and assurance that Personal Information disposed of by the customer through Mobile Banking is true, complete, and up to date. Further, the customer acknowledges and agrees that failure to provide up-to-date Personal Information required by Mobile Banking will result in certain inconveniences and restrictions of access to CCU Mobile's features.

b) Personal Information collected as part of customer identity can be held by CCU for the purpose of enabling customers to use the services provided by CCU.

c) CCU can collect any information on customer usage behavior for the purpose of security enhancements and user experience improvements.

d) CCU may require access to location data on customer's mobile device. This data can be used for enhancing the security of CCU Mobile, improving CCU services, and sending location-based offers.

e) CCU may check customer's mobile identity while customer register or activates CCU Mobile, updates personal information, or performs transactions, as part of security measures in using the Mobile Banking app.

12.2. CCU may also be required under certain legislation to disclose customer Personal Information and confidential information relating to the operation of the customer account, and the customer expressly consents to and agree to such disclosure.

12.3. Customer provide the express consent and agree that CCU may share customer Personal Information with third parties to comply with a legal obligation when CCU believes in good faith that applicable law requires it, at the request of governmental authorities pursuant to applicable law, to verify or enforce our contractual rights or other applicable policies, to detect and protect against fraud, or any technical or security vulnerabilities, to respond to an emergency, and/or so that third-parties, such as third party payment processors, can provide services necessary for CCU to provide any services under the Specific Terms and

Conditions. If there is any breach of customer information by a third party, the customer agrees to release CCU from any liability and pursue any legal action against such third party.

13. ADDITIONAL SPECIFIC TERMS AND CONDITIONS

13.1. Other functions like deposit, card, fund transfer, and other services customers access using CCU Mobile, and each transaction made in the account, remains subject to its specific terms and conditions governing those functions respectively.

14. INTELLECTUAL PROPERTY

14.1. CCU owns or has obtained a valid license to use all intellectual property used in connection with the provision of CCU Mobile. Information provided to customers as part of Mobile Banking may only be used for personal use and reference only and may not be reproduced, distributed, or transmitted to any person or incorporated into any other document without CCU's prior written consent.

15. AMENDMENTS

15.1. CCU may change the Specific Terms and Conditions at any time. If so, CCU will always give a customer a reasonable notice period required by applicable law and communicate these changes, either by direct communication, by display in CCU's branches, by notice in the media (including public notices), by notice on CCU's website or any other method of electronic communication used by the customer.

16. DISPUTE RESOLUTION AND GOVERNING LAW

16.1. Any dispute arising out of or in connection with the Specific Terms and Conditions, including any question regarding its existence, validity, performance, or termination, shall be referred to and finally resolved by arbitration in the Kingdom of Cambodia in accordance with the Arbitration Rules of the National Commercial Arbitration Center ("NCAC Rules") being in force at the time of commencement of arbitration and by reference in this clause the NCAC Rules are deemed to be incorporated as part of this contract. The Tribunal shall consist of one arbitrator. The language of the arbitration shall be English. The Specific Terms and Conditions are governed by the laws of Cambodia.

END!