Terms and Conditions for the use of the Biometric Authentication Service

By undergoing the registration process to use the Biometric Authentication Service, or using the Biometric Authentication Service, you accept and agree to these Terms and Conditions. If you do not accept these Terms and Conditions, please do not register for or access or use the Biometric Authentication Service.

1. Definitions and Interpretation

1.1. These terms and conditions ("Terms and Conditions") apply to and regulate your use of the Biometric Authentication Service provided by OCBC Bank (Macau) Limited (" the Bank" ).

1.2. In these Terms and Conditions, the following words shall have the following meanings:

"App" means the OCBC Bank Personal Mobile Banking Application (as updated from time to time) which can be downloaded to any mobile device which runs an operating system supported by the Bank, through which you can access the OCBC Bank personal Mobile Banking services;

"Biometric Authentication Service" means the identity authentication function using biometric credentials (including fingerprint, face authentication or any other biometric data), as the Bank may provide from time to time pursuant to these Terms and Conditions;

"Macau" means the Macau Special Administrative Region of the People's Republic of China; and

"Permitted Mobile Device" means such Apple device and compatible Android device running an operating system version as the Bank may specify from time to time, or any other electronic devices or equipment which the Bank may designate for using Biometric Authentication Service from time to time.

2. Biometric Authentication Service is provided as part of the OCBC Bank personal Mobile Banking services, and accordingly:

2.1. These Terms and Conditions are in addition to and shall be read in conjunction with the Bank's Terms & Conditions For All Accounts And Related Services. Please refer to https://www.ocbc.com.mo/file/account-and-related-services-terms-and-conditions_en.pdf

2.2. If there is any inconsistency between the provisions of these Terms and Conditions and the provisions of the Bank's Terms & Conditions For All Accounts And Related Services, the provisions of these Terms and Conditions shall prevail;

2.3. Terms used in these Terms and Conditions shall have the same meanings as defined in the Bank's Terms & Conditions For All Accounts And Related Services unless otherwise defined in these Terms and Conditions or the context requires otherwise.

3. Biometric Authentication Service provides an alternative to using personal mobile banking PIN to verify your identity for accessing the OCBC Bank personal Mobile Banking services via the App. You can register your Permitted Mobile Device (with biometric identity sensor supported) for Biometric Authentication Service. Once successfully registered, you may use your biometric credentials to confirm your identity for accessing the OCBC Bank personal Mobile Banking services via the App.

4. Having registered for Biometric Authentication Service, you may still choose to access the OCBC Bank personal Mobile Banking services via the App by using your personal mobile banking User ID and PIN.

5. You can deactivate the Biometric Authentication Service yourself at any time via the App. Once deactivated, you may continue to access the OCBC Bank personal Mobile Banking services via the App by using your personal mobile banking User ID and PIN. Please note that deactivation of the Biometric Authentication Service will not automatically delete your biometric credentials on your Permitted Mobile Device. Your biometric credentials will be continuously stored on your Permitted Mobile Device unless they are deleted by you through the relevant biometric authentication function on your Permitted Mobile Device. Biometric credentials stored on your Permitted Mobile Device may be used by other applications on your Permitted Mobile Device.

6. You acknowledge and agree that in order to use Biometric Authentication Service:

6.1. You must be a valid user of the OCBC Bank personal Mobile Banking services;

6.2. You must install the App using your Permitted Mobile Device;

6.3. You must activate the biometric identity sensor on the Permitted Mobile Device and register at least one of your biometric credentials to control access to the Permitted Mobile Device;

6.4. You confirm and authorize the Bank to verify your identity by biometric credentials registered on your Permitted Mobile Device instead of your OCBC Bank personal Mobile Banking User ID and PIN;

6.5. Upon successful registration for Biometric Authentication Service, all biometric credentials stored on the Permitted Mobile Device registered for Biometric Authentication Service at the time of or after registration can be used to access the OCBC Bank personal Mobile Banking services via the App. Therefore, you must ensure that only your own biometric credential is stored on the Permitted Mobile Device. If you store any other person's biometric credential or allow any other person's biometric credential to be stored on the Permitted Mobile Device, you are responsible for any person using the other biometric credential to access the OCBC Bank personal Mobile Banking services, including without limitation operating your accounts and effecting transactions. You agree that all such dealings and transactions will be deemed to be authorized by you and will be binding on you;

6.6. Each time the App detects the use of a biometric credentials registered on the Permitted Mobile Device registered for Biometric Authentication Service to access the OCBC Bank personal Mobile Banking services, you are deemed to have accessed the OCBC Bank personal Mobile Banking services;

6.7. The authentication is performed by the App by interfacing with the biometric identity sensor module on your Permitted Mobile Device and you agree to the authentication process. The Bank will not collect or store your biometric credentials in any manner at any stage of your registration or use of the Biometric Authentication Service;

6.8. You shall not use the App on any mobile device or operating system that has been modified outside the mobile device or operating system vendor supported or warranted configurations (e.g. devices that have been " jail-broken" or " rooted" ). A jail broken or rooted device means one that has been freed from the limitations imposed on it by the mobile service provider and/or the phone manufacturer without their approval. The use of the App or Biometric Authentication Service in a

jail- broken or rooted device is entirely at your own risk and the Bank will not be liable for any losses or any other consequences suffered or incurred by you as a result;

6.9. You shall not use face authentication for Biometric Authentication Service if you have an identical twin sibling, in which case you shall use the OCBC Bank personal Mobile Banking User ID and PIN to access OCBC Bank personal Mobile Banking services via the App;

6.10. You shall not use face authentication for Biometric Authentication Service if you are an adolescent while your facial features may be undergoing a rapid stage of development, in which case you shall use the OCBC Bank personal Mobile Banking User ID and PIN to access the OCBC Bank personal Mobile Banking services via the App; and

6.11. You shall not take any action to disable any function provided by, and/or agree to any settings of, your mobile device that would otherwise compromise the security of the use of your logon credentials for authentication purposes (e.g. disabling "attention- aware" for face authentication).

7. The Bank has the right to specify or vary from time to time the scope and features of Biometric Authentication Service without prior notice.

8. All instructions received by the Bank with your identity verified through Biometric Authentication Service shall be binding on you. You are liable for all such instructions and all resulting transactions in accordance with the provisions of the Bank's Terms & Conditions For All Accounts And Related Services.

9. The Bank has the right to modify, suspend or terminate Biometric Authentication Service or its use by you at any time without giving prior notice or reason where the Bank shall, in its absolute discretion, deem fit; and the Bank shall not be liable to you for all loss or damage that may be suffered by you.

10. The Bank reserves the right to amend, supplement, delete or replace at any time these Terms and Conditions, with or without giving prior notice in writing to you; and if the Bank, in its absolute discretion, decides to give such notice, such notice may be made in such manner and by such means of communication as the Bank shall deem fit. You acknowledge and agree that you shall observe and comply with any such amendment, supplement, deletion or replacement when using the Biometric Authentication Service. Your continued use of the Biometric Authentication Service shall constitute your acceptance of any such amendment, supplement, deletion or replacement.

11. Liabilities of the Bank

11.1. The biometric identity sensor module on your Permitted Mobile Device is not provided by the Bank. The Bank makes no representation or warranty as to the security of the Biometric Authentication Service function of any Permitted Mobile Device and whether it works in the way that the manufacturer of the Permitted Mobile Device represents or warrants;

11.2. The Bank does not represent or warrant that the Biometric Authentication Service will be accessible at all times, or function with any electronic equipment, software, infrastructure or other personal Mobile Banking services that the Bank may offer from time to time;

11.3. The Bank is not liable for any loss, damages or expenses of any kind incurred or suffered by you arising from or in connection with your use of or inability to use Biometric Authentication Service except any direct loss or damages caused solely by negligence or willful default on the part of us; and

11.4. Under no circumstances is the Bank liable for any indirect, special, incidental, consequential, punitive or exemplary loss or damages, including without limitation loss of profits, loss due to business interruption or loss of any programme or data in your Permitted Mobile Device.

11.5. Once a Permitted Mobile Device has been registered for the Biometric Authentication Service in respect of your OCBC Bank personal Mobile Banking, information about your OCBC Bank personal Mobile Banking can be accessed using the biometric credentials. The Bank owes no duty to verify that the relevant biometric credentials are your biometric credentials. All use and access of the OCBC Bank personal Mobile Banking services referable to any biometric credentials (whether such access or use is authorised by you or not) shall be deemed to be use or access of the OCBC Bank personal Mobile Banking services by you.

12. Law and Jurisdiction

12.1. These Terms and Conditions shall be governed by and construed in accordance with the laws of Macau.

12.2. You submit to the non-exclusive jurisdiction of the Macau courts.

13. Miscellaneous

13.1. Each provision of these Terms and Conditions is severable from the others. If at any time any provision is or becomes illegal, invalid or unenforceable in any respect, the legality, validity or enforceability of the remaining provisions shall not be affected in any way.

13.2. The Bank may assign or transfer all or any of its rights and obligations under these Terms and Conditions to any person without your prior consent.

13.3. The English version of these Terms and Conditions shall prevail wherever there is any inconsistency between the English and the Chinese versions.