Terms and Conditions for Mobile Security Key and Biometric Authentication for Banking Services

These Terms and Conditions govern your use of the Mobile Security Key and Biometric Authentication provided by the Hang Seng Bank Limited ("we", "us", "our", "Hang Seng"), and form part of the End User License Agreement between you and us governing the use of the Hang Seng Mobile App. Unless otherwise defined herein, capitalized terms herein shall have the same meanings as those defined in the End User License Agreement.

1. Definitions
    1.1 "Biometric Authentication" means the identity authentication function using biometric credentials (including fingerprint, iris, facial map or any other biometric data), as we may provide from time to time pursuant to this Agreement.
    1.2 "Mobile Security Key" means a feature within the App which is a software-based Security Device used to generate a one-time Security Code, as we may provide from time to time pursuant to this Agreement.
    1.3 "Permitted Mobile Device(s)" means such as Apple device and compatible Android device running an operating system version as we specify from time to time, or any other electronic devices or equipment which we may enable for using Mobile Security Key or Biometric Authentication from time to time.
2. Mobile Security Key
    2.1 Mobile Security Key provides an alternative means of verifying your identity for accessing the Services. You may register the Mobile Security Key on your Permitted Mobile Device(s) by completing the steps specified by us.
    2.2 Once successfully registered, you have to use the password associated with the Mobile Security Key on your Permitted Mobile Device(s) to confirm your identity for accessing the Services.
    2.3 You may also use Mobile Security Key to generate a one-time Security Code as a second verification when performing certain Personal e-Banking transactions which require the Security Code.
    2.4 You may deactivate Mobile Security Key at any time via the App by completing the steps specified by us. Once deactivated, you may not be able to continue to access the Services if Mobile Security Key is deemed necessary for accessing the services.
    2.5 We have the right to specify or vary from time to time the scope and features of Mobile Security Key without prior notice.
    2.6 You can set up Mobile Security Key on one or multiple (if applicable) Permitted Mobile Device(s) which we will identify by way of your mobile device ID.
3. Biometric Authentication
    3.1 Biometric Authentication provides an alternative to using your Mobile Security Key password to verify your identity for accessing the Services. You have to register your Permitted Mobile

Device(s) (with biometric identity sensor supported) for Biometric Authentication by completing the steps specified by us.

3.2 Once successfully registered, you may use your biometric credentials registered on the Permitted Mobile Device(s) to: confirm your identity for accessing the Services via the App; and to generate a one-time Security Code as a second verification when performing certain Personal e-Banking transactions which require the Security Code.

3.3 Having registered for Biometric Authentication, you may still choose to access the Services by using your Mobile Security Key password.

3.4 You may deactivate Biometric Authentication at any time by completing the steps specified by us. Once deactivated, you may continue to access the Services by using your Mobile Security Key password.

3.5 We have the right to specify or vary from time to time the scope and features of Biometric Authentication without prior notice.

4. Rights and Responsibilities

4.1 By registering the Mobile Security Key and/or Biometric Authentication, you authorise us to verify your identity by any Mobile Security Key or biometric credentials registered on your Permitted Mobile Device(s), and to verify your identity by the Mobile Security Key or biometric credentials registered on your Permitted Mobile Device(s) as a second verification for logging on to Hang Seng Personal e-Banking or performing Personal e-Banking transactions which require a one-time Security Code, as if each Mobile Security Key or biometric credential were a username, password, identifier, Security Code or other security code for identifying you for the purposes of accessing accounts, services or products under the Other Terms.

4.2 In order to use Mobile Security Key or Biometric Authentication:

4.2.1 you must be a valid user of the Services;

4.2.2 you must install the App using your Permitted Mobile Device(s);

4.2.3 you must register a password for the Mobile Security Key on your Permitted Mobile Device(s); and

4.2.4 (for Biometric Authentication) you must activate the biometric identity sensor on the Permitted Mobile Device(s) and register at least one of your biometric credentials to control access to the Permitted Mobile Device(s).

4.3 You fully understand and agree that:

4.3.1 upon successful registration for Biometric Authentication, ALL biometric credentials stored on the Permitted Mobile Device(s) registered for Biometric Authentication at the time of or after registration can be used to access the Services. Therefore, you must ensure that only your own biometric credential is stored on the Permitted Mobile Device(s). 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(s), you are responsible for any person using the

other biometric credential to access the Services, including operating your accounts and effecting transactions. All such dealings and transactions will be deemed to be authorised by you and will be binding on you;

4.3.2 each time the App detects the use of biometric credentials registered on the Permitted Mobile Device(s) registered for Biometric Authentication to access the Services, you are deemed to have accessed the Services; and

4.3.3 the authentication is performed by the App by interfacing with the biometric identity sensor module on your Permitted Mobile Device(s). We do not collect your biometric credentials. The App will access the biometric identity sensor in your Permitted Mobile Device(s) and obtain the necessary information to perform the authentication. You consent to the authentication process and our accessing and using the information obtained via the biometric identity sensor.

4.4 You should take all reasonable security measures to prevent unauthorised or fraudulent use of Mobile Security Key or Biometric Authentication, including the following measures:

4.4.1 you should take reasonable precautions to keep safe and prevent loss or fraudulent use of your Permitted Mobile Device(s), Hang Seng Personal e-Banking username and password, and the Mobile Security Key password. You should observe the security recommendations provided by us from time to time about the use of Mobile Security Key or Biometric Authentication;

4.4.2 you must not use the App, Mobile Security Key or Biometric Authentication on any mobile device or operating system that has been modified outside the mobile device or operating system vendor supported or warranted configurations. This includes 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 your mobile service provider and the phone manufacturer without their approval. The use of the App, Mobile Security Key or Biometric Authentication on a jail-broken or rooted device may compromise security and lead to fraudulent transactions. Download and use of the App, Mobile Security Key or Biometric Authentication in a jail-broken or rooted device is entirely at your own risk and we will not be liable for any losses or any other consequences suffered or incurred by you as a result;

4.4.3 you should not use facial recognition for Biometric Authentication if you have an identical twin sibling;

4.4.4 you should not use facial recognition for Biometric Authentication if you are an adolescent while your facial features may be undergoing a rapid stage of development

4.4.5 you should not take any action to disable any function provided by, and/or agreeing to any settings of, your mobile device(s) that would otherwise

compromise the security of the use of your biometric credentials for Biometric Authentication (e.g. disabling "attention-aware" for facial recognition); and

4.4.6 if you are aware of or suspect any unauthorised use of your Permitted Mobile Device(s) or Hang Seng Personal e-Banking username and password or Mobile Security Key password for effecting Mobile Security Key or Biometric Authentication, you should notify us as soon as reasonably practicable by calling our 24-hour Customer Service Hotline at 2822 0228. We may require you to change your Hang Seng Personal e-Banking username and password, re-register Mobile Security Key, re-register your biometric credentials or cease to use Mobile Security Key or Biometric Authentication.

4.5 All instructions received by us with your identity verified through the Mobile Security Key or Biometric Authentication shall be binding on you. You are liable for such instructions and all resulting transactions in accordance with the provisions of the Other Terms, including the provisions relating to your liability for unauthorised transactions if you acted fraudulently or with gross negligence.

4.6 We have the right to modify, suspend or terminate Mobile Security Key and/or Biometric Authentication or its/their use by you at any time without giving prior notice or reason where we reasonably consider necessary or advisable to do so. These cases may include actual or suspected breach of security.

5. Limitation of our Liability

5.1 Mobile Security Key or Biometric Authentication is provided on an "as is" and "as available" basis. We do not warrant that Mobile Security Key or Biometric Authentication will be available at all times, or that it will function with any electronic equipment, software, system or other Services that we may offer from time to time.

5.2 The biometric identity sensor module on your Permitted Mobile Device(s) is not provided by us. We are not responsible for the biometric identity sensor technology.

5.3 We are 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 Mobile Security Key or Biometric Authentication unless it is caused solely and directly by the negligence or willful default on our part or on the part of our employees or agents.

5.4 Under no circumstances are we liable for any indirect, special, incidental, consequential, punitive or exemplary loss or damages, including loss of profits, loss due to business interruption or loss of any programme or data in your Permitted Mobile Device(s).