General Descriptive Information – Online Banking Services

This document provides only general descriptive information on the use of the Online Banking Services (the "**Online Banking Services**") and it is solely prepared for your ease of reference. For more information, please refer to:

- Terms and Conditions for Accounts and Related Services (for individual),
- Terms and Conditions for Online Banking Services, or
- the Bank's website.

1. Fees and charges

- Fee and charges associated with the Online Banking Services, please refer to the Schedule of Service Fees (General Banking Services).

2. Personal data protection

- In relation to protection of customers' personal data under the Online Banking Services, please refer to the Notice to Customers relating to the Personal Data Ordinance and the Privacy Policy Statement.

3. Customer's undertakings and obligations

- The Customer shall undertake to use the Online Banking Services (including but without limitation to the Website, Mobile App, the Security Token and the Mobile Token) in accordance with the Terms and Conditions for Online Banking Services and the operation policy and procedure relating to Online Banking Services provided by the Bank from time to time.
- The Customer undertakes, among others:
    - not to tamper with, modify, decompile, reverse engineer or otherwise alter or gain unauthorised access to any part of the Online Banking Services, the Website, the Mobile App, the Mobile Token, or any of the software comprised in them;
    - not to access or use the Website, Mobile App, or Mobile Token on any 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 Website, Mobile App, or Mobile Token on a jail broken or rooted device may compromise security and lead to fraudulent transactions; and
    - to only download the Mobile App and its updates from the official mobile application online stores (e.g. Google Play / Apple App Store).
- The Bank is entitled to terminate the use of the Online Banking Services (including but without limitation to the Website, Mobile App, the Security Token and the Mobile Token) by the Customer without notice and to take legal action against the Customer for breach of the above undertakings.
- The Customer shall also be fully responsible and liable for all consequences arising from or in connection with the use of the Online Banking Services if he or she fails to take any of the security measures communicated or published by the Bank or his or her electronic devices' manufacturer from time to time.
- The Customer shall notify the Bank as soon as the Customer encounters any irregularity or difficulty in using any Online Banking Services.

- The Customer represents and warrants to the Bank that its use of the Online Banking Services will comply with all applicable laws, rules and regulations and the user guides, policies and procedures applicable to the Online Banking Services and these Terms and Conditions for Online Banking Services and any other agreement between the Customer and the Bank, as may be amended from time to time.

4. Customer's liability for unauthorized transactions

- Generally speaking, if there is no gross negligence, fraud or fault on the part of the Customer, such as failing to properly safeguard his or her device(s) for using the Online Banking Services (including but without limitation to the Website, Mobile App, the Security Token and the Mobile Token), the Customer will not be liable for any direct loss suffered by the Customer as a result of any unauthorised Online Banking Transaction.
- However, the Customer shall understand that there are risks of the Card, Username, Password, Mobile Token Password and Mobile Token (where applicable) and/or Security Code of the Customer being misused by unauthorised persons or used for unauthorised purposes. And the Customer shall notify the Bank as soon as reasonably practicable upon:
  - (i) any notice or suspicion of the Card, Username, Password, Mobile Token Password (where applicable), Security Token (where applicable), and/or Security Code being lost, stolen, compromised or disclosed to or obtained by any unauthorised person;
  - (ii) any unauthorised instruction given or transaction effected with the Card, Username, Password, Mobile Token Password (where applicable) and/or Security Code; or
  - (iii) any compromise or unauthorised use of the Mobile Token.
- If the Customer fails to report such incidents to the Bank as soon as reasonably practicable, or has otherwise acted fraudulently or with gross negligence, the Customer may be held responsible for all such transactions involving the use of any of the Card, Username, Password, Mobile Token Password (where applicable), Mobile Token (where applicable) and/or Security Code and all direct losses as a result.

Important Notice to Customer

- The Customer is responsible for all its acts and omissions and shall comply with the provisions of the relevant application form and the Terms and Conditions for Online Banking Services.
- Customers will be liable for all losses if they have acted fraudulently.
- Customers will be liable for all losses if they have acted with gross negligence (this may include cases where customers knowingly allow the use by others of their device or authentication factors) or have failed to inform institutions as soon as reasonably practicable after realizing that their authentication factors or devices for accessing the Online Banking Services have been compromised, lost or stolen, or that unauthorized transactions have been conducted.
- Customers will be liable for all losses if they fail to follow the safeguards set out in below:
  - i. Customers shall take reasonable steps to keep any device (for example, personal computers, security devices that generate one-time passwords and smart cards that store digital certificates) or authentication factors (for

example, passwords and authentication tokens) used for accessing Online Banking Services secure and secret.

ii. Customers have to take reasonable steps to keep the device safe and the authentication factors (for example, passwords) secret to prevent fraud.

iii. Among others, the Customers is advised:

a. that they should destroy the original printed copy of the passwords;
b. about the risks associated with the adoption of Biometric Credentials, Mobile Token or device binding as one of the authentication factors used for initiating relevant transactions (e.g. contactless mobile payments) and the relevant protection measures to secure the devices and authentication factors;
c. that they should not allow anyone else to use their authentication factors;
d. to change the Password and Mobile Token Password (where applicable) on a regular basis
e. never to write down the passwords on any device for accessing Online Banking Services or on anything usually kept with or near it;
f. not to write down or record the passwords without disguising them;
g. that they should notify the institutions as soon as practicable after they identify unusual or suspicious transactions on their accounts; and
h. of the need to ensure that their contact details registered with the institutions for the purpose of receiving important notifications from the institutions (for example, SMS and email notifications for online payments) are up-to-date to allow relevant notifications to be delivered to the customers on a timely basis.

- The Customer shall also be fully responsible and liable for all consequences arising from or in connection with the use of the Online Banking Services if he or she fails to take any of the security measures communicated or published by the Bank or his or her electronic devices' manufacturer from time to time.

5. <u>Security incident reporting</u>

- In the event of loss or theft of the Security Token or the mobile device to which a Mobile Token is bound, the Customer shall as soon as reasonably practicable notify such loss or theft to the Bank and confirm the same in writing if requested by the Bank.
- If the Customer fails to report such incidents as soon as reasonably practicable to the Bank or has otherwise acted fraudulently or with gross negligence, the Customer may be responsible for all direct losses as a result of all unauthorised transactions involving the use of, as the case may be, the lost Security Token or mobile device to which a Mobile Token is bound by any person. If a replacement Security Token or Mobile Token (where applicable) is issued, the Bank may charge a fee for it.
- Notice may be given by the Customer to the Bank via any of the following methods:
  i. calling the Bank's 24-hour customer hotline at +852 2779 5533, which is posted by the Bank in the Website or Mobile App;
  ii. contact any of the Bank's branches; or
  iii. any other method notified by the Bank from time to time.

In the event of any inconsistency between the English version and the Chinese version of this general descriptive information, the English version will prevail.