Safety Reminder of Using E-Banking

To protect your account security, we provide all the security measures and have system upgrades arranged. We recommend you to take the following measures to protect your online activities:

Keep your device safe and version up to date (applicable to Mobile Banking)

- Keep your mobile phone and UKey properly. You should contact us immediately for UKey replacement if you have lost the UKey.
- Only download official apps and updates published by CMBCHK. Please download apps at Apple App Store/ Google Play Store or official website www.cmbc.com.hk. Beware of all other download sources especially those embedded links via QR Code.
- Use secure networks help protect your information.
- To lower the risk, we recommend you to turn off functions allowing mobile payment such as Ali-pay and NFC functions when you are using Mobile Banking services.

Use secured machines and browsers (applicable to Internet Banking)

- Use a correct URL to access our Internet Banking services. You can directly key in our website www.cmbc.com.hk at the URL bar to access. Don’t login via links from emails, search engines or suspicious pop-up windows. Be reminded that we will not deliver emails with embedded links to Internet Banking services to our customers.
- You should install firewall and anti-virus software, regular update is necessary to avoid new viruses.
- Disable the ‘AutoComplete’ function to avoid auto form filling by browsers when you input credentials. You can open the browser and go ‘tools’ – ‘Internet Options’ – ‘Content’ – ‘AutoComplete Settings’ , uncheck ‘User names and passwords on forms’.

Protect your login credentials

- To secure your login credentials, we highly recommend that your login password and UKey passwords should contain more than 6 characters and a combination of numbers, alphabets and mixed capitalization, for example, Ci27Ld98.
- Always keep your user alias and passwords secure. Do not have them written down or shared. Keep your login information secret and do not reveal to anyone, including our staffs and the Police.
- Change your passwords regularly, 60-day is suggested.
- When you log in, make sure there is no one is around to watch your login alias and password on screen.
- Don’t provide any account related information to any other websites/ apps.

Logging in/ logging out

- We recommended you to use UKey for login. If you are logging in with a user alias, select a non-guessable combination and do not repeat your passwords sets.
- If you enter the wrong UKey password in error more than six times, your UKey will be disabled. You will need to contact us for a new UKey.
- If you have input the login password incorrect more than 5 times in the same day, you cannot login until the next day. The number of login password attempts is shared between Internet Banking and Mobile Banking.
- Every time you have logged in, we will be showing you the user alias, the last login channel, the last login date and time as well as the number of total login made on that day. If you find any information suspicious, please contact us immediately.
- We recommend you to choose receiving SMS notification every time you log in so you can view your login information.
- If there is no activity within a specified time, Internet Banking / Mobile Banking services will be automatically logged out. You have to login again if you want to use the online service.

- Remember to log out, disconnect the UKey and close the browser/ app after you have finished using our online services.

Keep your transaction safe and monitor your account

- Don’t perform any transactions at machines for public use.
- When making an authorisation for a transaction, you must check the details of the beneficiary account carefully. Input the UKey password only if you have verified the contents on UKey screen matches.
- A SMS will be sent to your mobile for the transaction confirmation and please verify the transaction details.
- In case of any change of your mobile numbers, please contact us the soonest to ensure the SMS can be received.
- Review your account balances and statements regularly to check if there is any suspicious transaction or unauthorised transaction.
- If you find any suspicious transaction or unauthorised transaction on your account, please contact us immediately.