交通銀行（香港）
BANK OF COMMUNICATIONS (HONG KONG)

Dear Customer,

Implementation of Two-factor Authentication for Precious Metals and Foreign Exchange Margin Trading Services

We commit to providing you with safe and secure Internet/Mobile Banking Services. To help you have better protection when using Internet/Mobile Banking Services, staring from15th November2024, customers will be required to use Mobile Token or Security Device for two-factor authentication ("2FA") for accessing our online precious metals and foreign exchange margin trading platform via Internet Banking and Mobile Banking Services .

Customers may download and install "BOCOM(HK) Mobile Banking" Apps through App Store, Google Play or the bank website to activate Mobile Token Service.

Important Notice

Protect your Personal Digital Keys; Beware of Fraudulent Links!

Internet banking login credentials, including usernames, login passwords and one-time passwords (OTPs), are as important in the digital world as the keys to their houses are in the physical one, and should be properly safeguarded.

In accordance with the HKMA's supervisory requirements, the bank will not send SMS or email messages with embedded hyperlinks directing customers to their websites or mobile applications to carry out transactions. Nor will the bank ask customers to provide sensitive personal information, including login passwords and OTPs, via hyperlinks.

If you receive SMS or email messages with embedded hyperlinks requesting you to input Corporate Internet Banking login credentials, these messages should not originate from the bank. You should think twice before clicking any hyperlinks purportedly sent by the bank, and contact the bank immediately if you have any concerns.

Exercise Caution with Mobile Applications

Please exercise utmost caution regarding malware that can manipulate your mobile device. When you are prompted to open suspicious links or download applications, it is crucial to proceed with caution. Before installing any applications, take the time to carefully evaluate the permission requirements of the respective mobile applications. If you come across any suspicious permission requests, it is advised not to install the related mobile applications. Unless you are completely certain, do not allow your system to install mobile applications from unknown sources.

Important Security Tips

1. Do not use the same password in accessing different online services. The password for accessing Internet/Mobile Banking Services should not be shared with other services.
2. Do check the last login details when you login Internet Banking/Mobile Banking Services. If you notice any suspicious login, please contact our Customer Services Hotline immediately at 223 95559.
3. If any unusual login screen or process (e.g. a suspicious pop-up window or request for providing additional personal information) was noted, customers are advised to stop login and log out immediately from the Internet Banking/Mobile Banking immediately and inform our Customer Services Hotline immediately at 223 95559.
4. Do not disclose banking details such as Internet Banking's usernames, passwords, one time passwords and other sensitive account information, to any third party providers, no matter authorized by the bank or not.
5. When using our Internet/Mobile Banking services, customers are advised to type the website address of BOCOM (HK) (www.hk.bankcomm.com) directly into the browser address bar or download and install Apps through App Store, Google Play or BOCOM (HK) website, for access to your Internet Banking or Mobile Banking accounts. Do not download software and apps from any untrusted sources.
6. If you have logged into our Internet Banking or Mobile Banking through third-party websites or third-party mobile Apps, you are advised to change the passwords immediately to protect your personal information. Customers who discover any unauthorized transactions in their bank accounts or have any queries relating to our Internet Banking or Mobile Banking Services should immediately contact our Customer Services Hotline at 223 95559.
7. Access Mobile Banking Services/ Securities Mobile Application by the recommended Operating Systems below:

Mobile Banking Services	Securities Mobile Application
iPhone with iOS 13.0 or above Mobile phone with Android 8.0 or above	iPhone with iOS 12.0 or above Mobile phone with Android 8.0 or above

8. You are advised to install the latest software updates for the Mobile Banking Services/ Securities Mobile Application.

9. To help the Customer stay vigilant against frauds, scams and deceptions, the Bank will send risk alerts based on the risk warnings, messages and indicators received by the Bank from “Scameter” provided by Hong Kong Police Force from time to time.

   (i) When you initiate fund transfers through FPS with FPS Proxy ID(mobile number/ email/FPS Identifier) of payees, if the FPS Proxy ID of payees are listed as High Risk on “Scameter”, risk alerts will be prompted before proceeding with the transactions. You will be asked to confirm whether you want to proceed with the transactions. Please be aware of such situations and follow the risk alerts to stop the transactions (if applicable) and be aware that the transactions are considered high-risk. If you choose to continue with the transactions, you will assume the associated risks and liabilities.

   (ii) You are encouraged to use “Scameter” provided by Hong Kong Police Force to conduct assessments of potential frauds and online security risks prior to making any fund transfers.

   (iii) When in doubt, you may call Anti-Scam Helpline 18222 for assistance or report to the Police.
10. Please exercise utmost caution regarding malware that can manipulate your mobile device. When you are prompted to open suspicious links or download applications, it is crucial to proceed with caution. Before installing any applications, take the time to carefully evaluate the permission requirements of the respective mobile applications. If you come across any suspicious permission requests, it is advised not to install the related mobile applications. Unless you are completely certain, do not allow your system to install mobile applications from unknown sources.
11. Please refer to the security advice provided by the Bank from time to time. The Bank will regularly review our security advice to ensure that it remains adequate and appropriate.

For other Internet Banking and Mobile Banking security guide, please read the Security Guide on the Bank’s website or the Security Tips in Mobile Banking App (Lifestyle > Services and Information > More > Security Tips).

If you have any queries, please contact our Customer Services Hotline at 223 95559.

Bank of Communications (Hong Kong) Limited (Incorporated in Hong Kong with limited liability)
(This is a computer print-out letter that requires no signature)