

Dear Valued Customer,

Information Security Reminder: Beware of Fraudulent SMS Messages

We are writing to draw your attention to the fraudulent SMS messages sent with Sender ID starting with the "#" sign.

At present, only the Registered Senders under the SMS Sender Registration Scheme (the "Scheme"), such as banks, telecommunications service providers, etc., can send SMS messages with Sender ID with prefix "#". However, it has been recently reported that members of the public have received suspected fraudulent SMS messages sent with Sender ID starting with "#" in an attempt to entice the SMS message recipient into believing that it were sent from a Registered Sender of the Scheme.

Upon receipt of suspicious SMS messages, please stay vigilant to the hyperlink(s) embedded and/or the phone number(s) provided in the message. In particular, you should neither click on any of hyperlinks embedded nor call any of phone numbers provided in the message. Besides, you should not respond to any of SMS messages which appear to be suspicious.

Please find below some useful security tips for dealing with suspected fraudulent SMS messages for your quick reference:

- I. Never disclose your personal information in response to the message.
- II. Never disclose your authentication factors for the Internet banking and/or mobile banking services (e.g. passwords, PINs, security codes, etc.) in response to the message. For the avoidance of doubt, our Bank and its staff will never ask you to provide your authentication factors under any circumstances.
- III. Never rely on the prefix "#" to determine the authenticity of an SMS message.
- IV. Always ignore the fund transfer request(s) raised in the message.
- V. Report to our Bank and the Police as soon as possible should you have been deceived by an SMS message (e.g. disclosure of your personal sensitive information, transfer of your money, etc. to the fraudster).

In case of doubt about the SMS messages spoofing our Bank's Sender ID, please feel free to contact our Customer Service Hotline (852) 2818 0282 for clarification, or check the Sender ID of the SMS message against our Bank's Sender ID registered with the registry of the Office of the Communications Authority https://www.ofca.gov.hk/en/consumer_focus/guide/hot_topics/ssrs/index.html.

Yours sincerely,
Shanghai Commercial Bank Limited

親愛的客戶：

資訊安全提示：警惕詐騙短訊

籲請 閣下留意以「#」號開頭的寄件者身份發送的詐騙短訊。

目前，只有在「短訊發送人登記制」（「登記制」）下登記的發送人，例如銀行、電訊服務供應商等，才可發送以「#」號為首的短訊。然而，最近有報告指出，公眾收到由「#」號開頭的寄件者身份發送的詐騙短訊，試圖誘使收件人相信該短訊是由該登記制下註冊的發件人發送。

如收到可疑短訊，請對短訊中嵌入的超連結和/或提供的電話號碼保持警惕。尤其不應點擊任何嵌入的超連結，也不應撥打訊息中提供的任何電話號碼。以及不應該回覆任何看似可疑的短訊。

以下是一些處理疑似詐欺性短訊的安全提示，供 閣下參考：

1. 切勿在回覆訊息時透露您的個人資料。
2. 切勿在回覆訊息時透露您的網上銀行和/或手機銀行服務的身份認證資訊（例如密碼、PIN、安全碼等）。為避免疑慮，本行及其職員在任何情況下均不會要求客戶提供身分認證資訊。
3. 切勿依賴「#」號來判斷短訊的真實性。
4. 忽略訊息中提出的資金轉移請求。
5. 如 閣下被騙（例如，透露了您的個人敏感資料、轉移了您的資金等），請盡快通知本行及警方。

如對發送人標註為本行的短訊有懷疑，歡迎致電客戶服務熱線 (852) 2818 0282 查詢，或經通訊事務管理局辦公室網頁 https://www.ofca.gov.hk/en/consumer_focus/guide/hot_topics/ssrs/index.html 對本行已登記的發送人識別碼進行核對。

上海商業銀行有限公司 謹啟