親愛的客戶您好，
Dear Customer,

【反詐騙提醒】
【Anti-fraud tips】

近年來歹徒會透過冒用快遞公司、政府機關、或銀行的名義，發送網絡釣魚電郵或偽冒手機短訊，企圖騙取您的個人資料、銀行帳戶或密碼。
There have been many cases of phishing scams through emails and SMS where fraudsters disguise as trustworthy institutions such as courier companies, government authorities, or banks in an attempt to obtain personal information, bank account, or passwords.

請注意本行不會透過手機短訊或預錄語音訊息電話，直接要求客戶提供其敏感資料，如身份證號碼、手機號碼、帳戶號碼等。
Please note that we will never directly request our customers to provide sensitive information, such as ID number, mobile phone number, or account number etc., through SMS or pre-recorded voice message phone calls.

客戶應對交易對手要求更改收款帳號之電郵保持警覺，應以其它聯絡管道(如電話)聯繫交易對手確認電郵的真偽性，以避免電郵詐欺事件發生。
Stay alert when receiving emails regarding the change of payment details from counterparty and use alternative communication channels (such as phone call) to confirm the email was truly sent by your counterparty to avoid the risk of fraud.

在收到任何聲稱代表銀行發出的電子郵件或來電時，請務必時刻保持警覺，並注意以下事項：
Upon receiving any emails or calls that purport to be from Mega ICBC Hong Kong Branch, customers must always be vigilant and pay attention to the following items:

- 定期檢查銀行戶口交易記錄；如發現有不尋常交易，請即與本行聯絡。
  Please check your bank statements regularly and contact us immediately if any abnormal transaction was found.
- 請勿向任何人透露您的電子銀行登入資訊，包括銀行或執法機構職員。
  Do not disclose your internet banking credentials to anyone, including the staff from banks or government authorities.
- 請勿將您的登入資訊儲存於裝置之中(如：iCloud鑰匙圈、Google密碼管理員)，或任何網路瀏覽器之自動儲存密碼或自動填補功能。
  Do not keep account information in your device such as iCloud Keychain, Google Password Manager, or use any password saving or auto fill function in the browsers.
- 確保您的密碼是獨一無二的，與您在其他服務的密碼不同；請定期更新您的密碼，切勿使用證照號碼、生日或電話號碼等資料做為密碼。
  Please make sure using a password different from other services. The login password should be changed regularly. Do not use ID number, date of birth or phone number as your password.
- 僅從官方應用程式商店下載並安裝由受信任且經過驗證的開發人員提供的應用程式；安裝前仔細評估應用程式請求的權限；並保持行動裝置的安全配置(如：禁止安裝來源不明的應用程式等)。
  Only download and install Apps provided by trusted and verified developers from official Apps stores; evaluate Apps' requested permissions carefully before installation; and maintain proper security configuration of mobile devices (e.g. disallow installation of Apps from unknown source, etc.).
- 請注意偽冒本行的短訊、電郵，切勿隨便回覆、點擊任何連結或打開任何附件；瀏覽網站時，請慎防仿冒本行的網站並切勿提供個人資料。
  Please do not reply any phishing SMS and suspicious e-mails, and do not click any hyperlink or open any attachment; please also be alert to the phishing websites and do not provide personal data.

如有任何懷疑請勿提供個人資料，並盡快致電本行：(852)2525-9687 分機 214、228、237，或撥打18222香港警方之反詐騙專線報案，或登入香港警方提供之防騙視伏器：https://cyberdefender.hk/scameter 查詢收款人相關資訊。
If you receive any suspicious messages, please do not disclose your personal information, and immediately contact us: (852)2525-9687 Ext. 214, 228 or 237, or dial 18222 Anti-Scam Helpline of the Hong Kong Police Force,or visit "https://cyberdefender.hk/scameter" of the Hong Kong Police Force to query payee related information.