

國泰君安國際已參與「短訊發送人登記制」及 防騙資訊

尊敬的客戶：

有關參與「短訊發送人登記制」

為協助市民識別短訊發送人的身分及防止墮入釣魚短訊詐騙的陷阱，香港通訊事務管理局辦公室（「通訊辦」）已實施「短訊發送人登記制」。

謹此通知，國泰君安國際控股有限公司（「本集團」）已加入由通訊辦推出的「短訊發送人登記制」，本集團旗下公司向香港登記手機號碼的客戶*所發出的單向短訊會使用已登記發送人名稱「#GTJAI」。

*現階段僅適用於國泰君安證券(香港)有限公司及/或國泰君安期貨(香港)有限公司持有香港登記手機號碼的客戶，而國泰君安外匯有限公司持有香港登記手機號碼的客戶將另行通知推出日期

請注意，短訊發送人登記制並不適用於：

1. 可供接收者以發送人號碼直接回覆的雙向短訊；
2. 使用非香港營辦商提供之一卡多號 / 一卡雙號流動服務的本地用戶；及
3. 香港以外的地區或國家的手提電話號碼。

相關通訊事務管理局辦公室「短訊發送人登記制」資訊請見以下網頁連結：

https://www.ofca.gov.hk/tc/consumer_focus/guide/hot_topics/ssrs/index.html。登記制的參與者會被記錄在通訊辦所建立的登記冊內，客戶可查閱該登記冊或直接聯絡本集團，以核實短訊發送人的身分及短訊的真實性。

有關防騙資訊

近期出現不少騙徒仿冒金融機構，向其客戶發出含有詐騙超連結的短訊，以獲取客戶資料並登入客戶帳戶進行未經授權交易，最終令客戶蒙受財務損失。為保障客戶戶口及資金安全，本集團特此提醒所有客戶及投資者注意並保持警惕，謹防受騙，敬請客戶注意以下事項：

1. **不透過電子訊息發送超連結引導登入** - 本集團旗下公司不會透過電子訊息(包括手機短訊及電子郵件等)發送超連結引導客戶以登入其交易帳戶，因此本集團發出的真實短訊將不內含任何超連結，客戶可以直接訪問本集團官方網站或透過流動應用程式登入交易帳戶。
2. **保持警覺** - 客戶即使收到以“#”號開頭的短訊，仍應保持警覺，及不應點擊任何內含的超連結。客戶如不慎點擊內含的超連結，及因而被引導至任何網站或流動應用程式的話，切勿輸入任何敏感或機密的個人資料，例如用作登入帳戶所需的用戶資料及一次性密碼。
3. **定期檢查帳戶活動** - 客戶應定期查核在本集團旗下公司開立的帳戶有關的任何活動，例如查閱交易帳戶登入、密碼重置、交易執行或帳戶資料變更通知等，以及時察覺或識別任何異常活動。
4. **開啟互聯網交易執行及系統登入通知** - 本集團建議客戶開啟互聯網交易執行及系統登入通知，讓客戶可儘早了解交易帳戶的登入及交易狀況，及時偵測所有潛在的未經授權交易，從而採取措施以降低或紓減與互聯網交易相關的黑客入侵風險，以保護客戶的交易帳戶。如已選擇不接收交易執行或系統登入通知的客戶可隨時選擇接收該等通知。
5. **值得信賴的防詐騙資源** - 客戶可以善用以下網站或 App 以獲得更加值得信賴或可靠的資訊或資源：



國泰君安國際
GUOTAI JUNAN INTERNATIONAL

- I. 「防騙視伏器」(<https://cyberdefender.hk/scameter/>)，網站以查核某網站、電話號碼、電郵等是否可能涉及欺詐
- II. 「防騙視伏 App」如偵測到用戶嘗試瀏覽可能涉及欺詐的網站，可實時向用戶發出警示
- III. 證監會警示名單(https://www.sfc.hk/TC/alert_list)
- IV. 守網者 (<https://cyberdefender.hk/>)
- V. 反詐騙協調中心 (<https://www.adcc.gov.hk/zh-hk/home.html>)
- VI. 投資者及理財教育委員會 (<https://www.ifec.org.hk/web/tc/index.page>)

如客戶懷疑自己的帳戶曾發生未經授權交易，應立即聯絡本集團客戶服務部，並請在適當情況下向香港警方報案。若客戶對任何可疑訊息存在疑慮，亦歡迎直接聯繫本集團客戶服務部進行核實，以確保個人資料與資金安全不受威脅。感謝客戶一直以來對本集團的信賴與支持，我們將持續致力於提升服務水準，為客戶提供更安全、便捷的資訊溝通平台。

如有任何疑問，請與本集團客戶服務部聯絡(熱線:40080 95521 /(852) 2509 7524，電郵: customer.service@gtjas.com.hk)。

國泰君安國際控股有限公司

2025 年 8 月 15 日

Guotai Junan International participation in the "SMS Sender Registration Scheme" and anti-fraud information

Dear Valued Clients,

Re: Participation in the SMS Sender Registration Scheme

In order to help residents verify the identities of SMS senders and to prevent the public from falling victim to phishing SMS scams, the Hong Kong Office of the Communications Authority ("OFCA") has implemented the "SMS Sender Registration Scheme" ("Scheme").

We are pleased to inform you that Guotai Junan International Holdings Limited ("the Group") has registered under OFCA's SMS Sender Registration Scheme and is now recognized as an "Accredited Sender". One-way SMS sent by subsidiaries of the Group to clients* with Hong Kong-registered mobile numbers will display the registered sender name "**#GTJAI**".

* Only available to clients with Hong Kong-registered mobile number of GUOTAI JUNAN SECURITIES (HONG KONG) LIMITED and/or GUOTAI JUNAN FUTURES (HONG KONG) LIMITED currently, and the launch date for clients with Hong Kong-registered mobile number of GUOTAI JUNAN FX LIMITED will be notified separately.

Please note that the Scheme does not apply to:

1. SMS messages of which receiving parties are expected to reply to the senders via phone numbers (two-way SMS);
2. Local subscribers of Single-Card-Multiple-Numbers / One-Card-Two-Numbers mobile service provided by non-Hong Kong operators; and
3. Mobile numbers registered outside Hong Kong.

For more details on OFCA's SMS Sender Registration Scheme, please visit:

https://www.ofca.gov.hk/en/consumer_focus/guide/hot_topics/ssrs/index.html . Registered participants of the Scheme are recorded in a register established by OFCA and you may either refer to this register or contact us directly to verify the sender's identity or the authenticity of the SMS messages.

Anti-Fraud Reminder

Recent incidents have involved fraudsters impersonating financial institutions to send SMS containing malicious hyperlinks, with the aim of capturing personal login credentials and executing unauthorized trades, resulting in financial loss to victims. To safeguard your account and assets, please remain vigilant and observe the following precautions:

1. **No Hyperlinks re-directing for login via Electronic Messages** - We will **never** send you a hyperlink by electronic messages (including SMS and emails) which re-direct you to log into your

trading account. As such, genuine SMS from us will not contain any embedded hyperlinks.

Always access your account by visiting our official website or mobile application directly.

2. **Remain Vigilant** - Even if you receive SMS with the prefix “#”, you should remain vigilant and not click on any embedded hyperlinks. If you accidentally click on the embedded hyperlinks and are thus redirected to any websites or mobile applications, you should not enter any sensitive or confidential personal information, such as user credentials and OTPs for logging onto your account.
3. **Regular Account Activity Checks** - Periodically review all account-related notifications—such as login alerts, password reset messages, trade execution notices and account-data change alerts—to detect any unusual activity promptly.
4. **Enable Internet-Trading Execution and System Login Notifications** - We strongly recommend you activate real-time notifications for trade executions and system login. Early notification helps you identify any unauthorized transactions swiftly so that you can take measures to mitigate hacking risks and protect your trading account. Where you have chosen to opt out of receiving trade execution or system login notifications, you may always choose to opt in of receiving such notifications.
5. **Trusted Fraud-Prevention Resources** - You may consult the following websites and mobile apps for reliable fraud-detection information and resources:
 - I. Cyber Defender Scameter (<https://cyberdefender.hk/en-us/scameter>), to verify whether a website, telephone number, or email address may be involved in fraudulent activities
 - II. “Scameter+” Mobile App, which can issue real-time alerts if it detects that you are attempting to visit a potentially fraudulent website.
 - III. Securities and Futures Commission Alert List (https://www.sfc.hk/en/alert_list)
 - IV. Cyber Defender (<https://cyberdefender.hk/en-us>)
 - V. Anti-Deception Coordination Centre (<https://www.adcc.gov.hk/en-hk/home.html>)
 - VI. Investor and Financial Education Council (<https://www.ifec.org.hk/web/en/index.page>)

If you suspect any unauthorized trading activity in your account, you should promptly contact our Customer Services Department, and please report it to the Hong Kong Police as appropriate. Should you have any doubts about any message you received, please contact our Customer Service Department immediately for verification to ensure the security of your personal data and funds. We appreciate your continued trust and support. We remain committed to enhancing our service standards and providing you with a secure and convenient communications platform.

Should you have any questions, please contact our Customer Services Department (CS Hotline: 40080 95521 / (852) 2509 7524) or email to customer.service@gtjas.com.hk.

Guotai Junan International Holdings Limited

15 Aug 2025