

4 May 2018

Circular to intermediaries

Receiving client orders through instant messaging

The Securities and Futures Commission (SFC) received a number of enquiries from the securities industry about the receipt of client orders through instant messaging¹ (IM). This circular provides guidance on the key controls and procedures which intermediaries are expected to put in place when using IM applications to receive client orders.

The use of IM technology poses new supervisory and record-keeping challenges. Most IM service providers do not provide users with tools to save, retrieve or monitor IM communications. Before allowing the use of IM applications to receive client orders, intermediaries should properly understand their features and limitations and carefully assess the risks involved.

Intermediaries which introduce IM technology into their business practices should put in place adequate measures and controls to ensure compliance with statutory and regulatory requirements, including the requirement to keep proper records of client orders². Complete and accurate records are an integral part of the audit trail. They ensure that reliable evidence is available to assess disputes with clients about the particulars of a trade order, and this protects the interests of both the intermediary and the client. For both the SFC and intermediaries, proper records also serve as a useful supervisory tool to detect irregularities and potential malpractices.

Intermediaries which allow the use of IM applications to receive client orders should implement appropriate measures which cover the following areas.

1. Centralised record keeping

- a) Messages relating to client orders (order messages) and the IM accounts and devices for storing and processing them should be properly maintained and centrally managed to reduce the possibility of error and minimise the risk of record tampering.
- b) Appropriate arrangements should be in place and sufficient capacity should be available to store and back up order messages in a form which could not be inappropriately modified or erased.
- c) All order messages should be fully recorded and properly maintained for a period of not less than two years³.

¹ IM is a form of electronic communication which allows two or more users to immediately transfer text messages and electronic files, such as images, audio, video and textual documents, across a network connection of mobile devices or computer platforms. Examples of major IM tools include WhatsApp and WeChat.

² The Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (Code of Conduct) and the Securities and Futures (Keeping of Records) Rules (Keeping of Records Rules).

³ Under Sections 3(1) and 10(b) and Section 1(d) of the Schedule to the Keeping of Records Rules, intermediaries are required to keep records showing the particulars of all orders or instructions which they received or initiated for no less than two years.



2. Security and reliability

- a) The identities of clients who send order messages should be properly authenticated and validated⁴. In case of doubt, direct confirmation should be obtained by calling clients at their registered phone numbers. Where appropriate, intermediaries should obtain a written acknowledgement from the client that order messages received via his mobile phone number originate from the client.
- b) Intermediaries should keep abreast of threat intelligence and fraud trends relating to IM applications and ensure that adequate and appropriate security safeguards⁵ are implemented to prevent unauthorised access or security attack. These safeguards should cover end-to-end data transmission as well as the IM accounts and devices used for storing and processing the order messages. The highest level of security available in the IM applications should be activated where appropriate.
- c) Client instructions received through IM applications for fund transfers to a third party account should only be approved on an exceptional basis after authentication of the identities of clients such as by making proper enquiries with clients through a different communication channel.
- d) A written contingency plan should be established to cope with emergencies and disruptions relating to IM applications. The contingency plan should be appropriately tested, regularly updated and communicated to clients.

3. Compliance monitoring

- a) All order messages should be readily accessible and appropriate equipment and facilities should be available for compliance monitoring and audit purposes.
- b) Regular compliance reviews should be performed to compare order messages against their clients' account activities to detect irregularities and potential malpractice.
- c) Intermediaries should ensure proper monitoring of unusual or questionable transactions, such as changes in trading patterns or trading large volumes of low turnover stocks, and verify them with clients where appropriate.

4. Internal policies and procedures

- a) Intermediaries should put in place written policies and procedures for the use of IM applications to receive client orders and these should be clearly communicated to staff. Monitoring procedures should be put in place to ensure that client orders received through IM applications are executed promptly.
- b) Staff members should be prohibited from making, sending or receiving electronic communications relating to client orders unless the intermediary has full control over the recording and retention of order messages.
- c) Appropriate and adequate training should be provided to staff regarding internal policies and procedures, regulatory requirements and security precautions⁵ for using IM applications for receiving client orders.

⁴ For example, intermediaries may authenticate a client's identity by requiring him to provide correct answers to some dynamic questions relating to his account and previous transactions, and not only to static questions.

⁵ Please refer to the guidelines published by the Hong Kong Computer Emergency Response Team Coordination Centre (www.hkcert.org/my_url/guideline/15033101), the Government of the Hong Kong Special Administrative Region (www.infosec.gov.hk/english/yourself/instant.html) and the Hong Kong Police Force (www.police.gov.hk/ppp_en/04_crime_matters/adcc/alert_180403_01.html) for reference.



5. Client awareness

- a) Intermediaries should take appropriate steps to raise the security awareness of their clients and ensure that they fully understand all the potential security risks⁵, such as phishing, malware, account theft and impersonation, as well as operational risks⁶, before allowing them to use IM applications to place orders. It may not be suitable for clients with inadequate security awareness to place orders through IM applications.
- b) The terms and conditions⁷ for using IM applications to place orders should be fully communicated and agreed with clients.

For reference, an example illustrating the use of IM applications to receive client orders is provided in the Appendix. Intermediaries may deploy other appropriate solutions according to their specific circumstances.

Intermediaries should prohibit their staff members from receiving client orders through IM applications if the above requirements are not fully met. The SFC will not hesitate to take regulatory action against intermediaries which use IM applications to receive client orders without putting in place sufficient measures to ensure compliance with the regulatory requirements.

Should you have any questions regarding the contents of this circular, please contact Ms Denise Chan at 2231 1188 or the case officers in charge.

Intermediaries Supervision Department
Intermediaries Division
Securities and Futures Commission

Enclosure

End

SFO/IS/025/2018

⁶ For example, the risks that order messages may not be delivered to the recipient in a timely manner and the IM applications may be out of service due to system or network problem.

⁷ For example, how to deal with situations which may give rise to potential disputes with clients; whether to require clients not to delete or recall delivered order messages; whether to acknowledge receipt of clients' order messages in a specific manner (eg, by copying and repeating clients' original order messages in the reply); the liabilities and responsibilities of clients and intermediaries in the event of fraud or unauthorised transactions; and specific contingency measures to deal with emergencies and disruptions relating to IM applications.