HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C
B9/29C

26 May 2016

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Security controls related to Internet banking services

I am writing to require authorized institutions (AIs) providing Internet banking services to further strengthen their security controls, having regard to recent incidents involving unauthorised share trading transactions.

In April this year, the Hong Kong Monetary Authority (HKMA) received reports from banks that the security of some customers' Internet banking accounts was compromised and unauthorised share trading transactions were conducted over these accounts. No fund transfers to unregistered third parties, which require two-factor authentication (2FA), were detected, although the affected customers must have been inconvenienced. On receipt of these reports, the HKMA issued on 20 April 2016 an E-banking Alert to draw the public's attention to this type of frauds. We have also held a series of discussions with AIs on ways to further strengthen the security controls over Internet banking services, with particular regard to share trading transactions.

In the light of these recent cases, the HKMA expects AIs providing Internet banking services to enhance their fraud monitoring mechanisms so as to keep up with new and emerging threats and fraudulent schemes. It would also be useful for AIs to send timely notifications (e.g. via SMS messages, e-mail or instant message services) to customers after each share trading transaction, so as to enhance the fraud monitoring process. Moreover, AIs should step up their efforts in raising customers' awareness of the security precautions that customers should take in order to mitigate the risks of these incidents. In addition, AIs should conduct a review of their security controls over Internet banking services to ensure that these controls remain robust and adequate to protect their customers' interests. Taking into account the feedback received from AIs, the HKMA considers the following additional measures to be useful in preventing and detecting the recent type of fraud cases:

(a) offering an option to customers to use 2FA to authenticate their identities before performing Internet share trading transactions, with appropriate disclosure to customers about the risk and implications of their choices. Such option should only be made or changed through a secure channel;

(b) offering an option to customers to set a daily limit on the volume of Internet share trading transactions that can be performed over their accounts;

(c) enforcing the use of difficult-to-guess Internet banking passwords;

(d) requiring customers to change their Internet banking passwords on a regular basis;

(e) stepping up the monitoring of unusual Internet banking access attempts and transactions (e.g. logins from Internet Protocol (IP) addresses or devices different from the usual ones used by customers or logins from suspicious IP addresses or locations) and sending notifications to customers whenever any such activities are detected; and

(f) implementing a challenge-response test during Internet banking login (or other effective measures) to counter automated brute-force attacks if 2FA is not used for logins into Internet banking services.

The HKMA expects AIs providing Internet banking services to implement, as soon as practicable, a combination of the above measures, together with any other effective steps, to strengthen their security controls. In the course of its ongoing supervision of AIs, the HKMA will assess whether AIs have in place adequate security controls to safeguard their safety and soundness and protect customers' interests.

Should you have any questions about this letter, please feel free to contact Ms. Teresa Chu at 2878 1563 or Mr. Tsz-Wai Chiu at 2878 1389.

Yours faithfully,

Raymond Chan
Executive Director (Banking Supervision)