HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C
B9/81C

5 June 2014

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Control measures for guarding against some recent fraud cases

I am writing to draw the attention of your institution to the modus operandi of some fraud cases reported in the past months and certain sound operational control measures for guarding against those cases.

Frauds of unauthorized fund transfers related to fake email/remittance instructions

According to the observations of Commercial Crime Bureau of the Hong Kong Police Force, one of the frauds reported in the past months warranting banking industry's specific attention was unauthorized fund transfers related to fraudulent email instructions. Typically, such email instructions were sent from fraudsters purporting to be the relevant authorized institutions' (AIs) customers by using email addresses similar to those of customers or by gaining unauthorized access to the customers' email accounts. After receiving the email instructions, the AIs concerned either did not call back the customers concerned or did not carry out their call back procedures robustly to verify the genuineness of the email instructions before processing the fund transfers.

The HKMA has also received reports that fraudsters submitted fictitious outward remittance instructions to AIs after getting hold of the victims' personal information (e.g., bank account numbers and HKID card numbers) by stealing the victims' letters from their mail boxes with lax security measures and then conducting searches in public registry (such as the Land Registry/Companies Registry for specimen signatures). While the AIs concerned did call back the customers to confirm the instructions, the fraudsters had managed to divert the calls to their phones through activating the call forwarding function[1]. As the AIs' call-back confirmation procedures were not stringent enough or not properly carried out by relevant staff, the fraudsters were able to answer the verification questions.

In the light of these frauds, the HKMA has conducted a series of thematic desktop reviews and on-site examinations to assess the related controls of selected AIs, particularly those

[1] These incidents highlight the importance that the authentication and related controls for activating call forwarding implemented by mobile network operators should be robust enough to prevent or detect unauthorized forwarding by fraudsters. The relevant staff of AIs should also remain vigilant in conducting call-back confirmation via the pre-registered telephone numbers provided by customers.

related to handling fund transfer instructions received from e-mail or fax. Based on the review results, the HKMA has identified some sound control practices (at **Annex**) for preventing and detecting such frauds, particularly:

(i) AIs should give serious consideration to not accepting third-party fund transfer instructions via emails. Even in the case that an AI considers such email instructions acceptable, such flexibility should only be available in very limited cases and they should also be covered by adequate compensating controls. In general, it is difficult for AIs to verify the genuineness of email instructions received via the internet. Moreover, any acceptance of email instructions from customers also exposes the customers to the risk of leakage of their authorized signatures shown in any email attachments. This would be highly undesirable, especially if the AI has not reminded the customers of the relevant risks;

(ii) In addition to signature verification controls, AIs should put in place further controls to confirm the genuineness of third-party fund transfer instructions received through email or fax before execution. In general, AIs should call back the relevant customer via a pre-registered telephone number provided by the customer to confirm the submission of such instruction. In case a threshold of fund transfer amount is set for mandatory call-back confirmation, the threshold amount should be commensurate with the risk appetite of the relevant business line. For fund transfers associated with a higher risk (e.g. large fund transfer amount), AIs should take further compensating controls;

(iii) AIs should establish clear policies and procedures on controls for guarding against fraudulent third-party fund transfers concerned. Apart from AIs' periodic internal audit reviews, the relevant business lines should also conduct on-going sample checks to ensure that the required controls are properly implemented by their staff.

We expect AIs to give full consideration to the sound control practices when evaluating and strengthening, where appropriate, their existing controls for guarding against the relevant frauds, having regard to their risk assessment, the service needs of their customers and the latest market developments.

<u>Frauds of unauthorized cheques withdrawals</u>

Another fraudulent technique noted involves the submission of falsified instructions to a bank in order to change the victim's correspondence address and then to request for a new cheque book to be mailed to the new address. We understand that the Hong Kong Association of Banks (HKAB) issued a circular on 19 May 2014 to provide a number of good practices in handling customers' requests for new cheque books received by mail, including calling the customer concerned to verify the request or seeking documentary proof where necessary, and notifying the customer by SMS, email or post after the request has been processed. The HKMA expects banks to adopt these good practices to enhance their security procedures.

<u>Card-Not-Present (CNP) credit card frauds</u>

We noticed that another fraudulent technique involves conducting CNP credit card transactions (e.g., payments over internet, telephone, physical mail, etc. without physical presentment of credit cards) by fraudsters using stolen credit card information. Although the card issuing banks sent SMS notifications to the cardholders' pre-registered mobile phone numbers, the fraudsters had managed to forward the SMS to their mobile phone numbers and the SMS notifications could not reach the cardholders' mobile phone numbers.

To help cardholders to detect similar frauds, the HKMA has discussed the matter with the HKAB, which in turn reached an agreement with mobile network operators to shortly implement a strengthened control. In particular, SMS notifications related to CNP transactions sent by credit card issuing banks will be sent to both the cardholders' pre-registered mobile phone numbers and any mobile phone numbers to which the SMS notifications have been forwarded (if the SMS forwarding services have been activated).

Should you have any question on the above-mentioned controls, please do not hesitate to contact Mr Parry Tang at 2878 1524 or Mr Alex Lee at 2878 1484.

Yours faithfully,

Henry Cheng
Executive Director (Banking Supervision)

Encl.

Annex

Examples of sound control practices related to fake email / remittance instructions

Controls related to acceptance of third-party fund transfer instructions received via email or fax

1. AIs should give serious consideration to not accepting third-party fund transfer instructions via email. Even in the case that an AI considers such email instructions acceptable, such flexibility should only be available in very limited cases and they should also be covered by adequate compensating controls. In general, it is difficult for AIs to verify the genuineness of email instructions received via the internet. Moreover, any acceptance of email instructions from customers also exposes the customers to the risk of leakage of their authorized signatures shown in any email attachments. This would be highly undesirable, especially if the AI has not reminded the customers of the relevant risks.

2. AIs should not accept third-party fund transfer instructions via fax unless they have received customers' written consents.

3. Before accepting a customer's request to use an email or a fax as a channel for submitting third-party fund transfer instructions, AIs should remind the customer of the possible risks associated with the channel, in line with the principle of maintaining a fair and cordial relationship with their customers. AIs should maintain documentation about such reminders given to customers.

Controls related to acceptance of remittance instructions received from non-account holders

4. AIs may give customers the flexibility to pre-register designated non-account holders who are allowed to submit remittance instruction forms in person for third-party fund transfer on behalf of the customers. Where a remittance instruction form for third-party fund transfer is received from a non-account holder (regardless of whether he or she has been pre-registered by the customers), the AI should consider whether to verify his or her identity (e.g. by sight of the HKID card or passport) and record the relevant identity information if permitted under the Personal Data (Privacy) Ordinance for the purpose of crime prevention or detection.

Controls related to confirming third-party fund transfer instructions

5. In addition to signature verification controls, AIs should put in place further controls to confirm the genuineness of third-party fund transfer instructions received through email or fax before execution[1]. In general, AIs should call back the relevant customer via a pre-registered telephone number provided by the customer to confirm the submission of such instruction.

---

[1] As third-party fund transfer instructions received via post or submitted via branches by non-account holders could also be subject to fraud risk, AIs should also implement additional controls for confirming such instructions that are of a higher risk before execution.

6. In case a threshold of fund transfer amount (which may vary among channels/business lines) is set where call-back confirmation is mandatory only if the transfer amount of the third-party fund transfer instruction exceeds the predetermined level, the threshold amount should be commensurate with the risk appetite of the relevant business line. It should also be reviewed and endorsed regularly by the senior management or relevant risk committees of the AI.

7. AIs should specify the criteria and factors for identifying third-party fund transfer instructions of particularly higher risk. For instance, these may include instructions involving a large transfer amount or unusual payment pattern or payees received via e-mail or remittance instructions received from non-account holders who have not been pre-registered. For fund transfers associated with particularly higher risk, AIs should take further compensating controls, such as:

   (a) where applicable, assigning a staff member (e.g. a relationship manager) who knows the relevant personal customer very well to conduct the call-back confirmation via a pre-registered telephone number[2]. If the staff member is unable to recognise the relevant customer, he or she should consider asking dynamic questions[3] where practicable, in addition to static questions, during call-back confirmation;

   (b) contacting pre-registered person(s) of corporate customers to conduct the call-back confirmation via pre-registered telephone number(s). If the fund transfer involves a very large value or there is suspicion, AIs should consider taking further practicable steps to confirm the instruction.

Controls related to awareness of relevant staff and periodic audits and reviews

8. AIs should establish clear policies and procedures, which should be subject to regular reviews, on the above-mentioned and any other relevant controls for guarding against fraudulent third-party fund transfers concerned. AIs should also periodically raise the awareness among relevant staff of these policies and procedures.

9. Apart from AIs' periodic internal audit reviews, the management of relevant business lines should also conduct on-going sample checks to ensure that the required controls are properly implemented by their staff.

---

[2] Some fraud cases highlight the importance that the authentication and related controls for activating call forwarding implemented by mobile network operators should be robust enough to prevent or detect unauthorized forwarding by fraudsters. The relevant staff of AIs should also remain vigilant in conducting call-back confirmation via the pre-registered telephone numbers provided by customers.

[3] Following the same principle, certain banks send a SMS message containing a one-time verification code to the customer of a remittance instruction received from non-account holders and then require the customer to provide the code during call-back confirmation.