HONG KONG MONETARY AUTHORITY
香港金融管理局

Banking Supervision Department

Our Ref : B1/15C
B9/81C

25 February 2015

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

The Hong Kong Monetary Authority published today the enclosed second issue of Operational Incidents Watch.

The Operational Incidents Watch is a periodic newsletter to share with the industry the major lessons learnt from selected significant operational incidents that have happened in the banking sector. It aims at facilitating authorized institutions (AIs) and the members of the public in Hong Kong to stay alert and to take appropriate measures to prevent similar incidents from happening to them. In this connection, we expect AIs' senior management to ensure that their relevant business lines and operational risk management functions will take into account the Operational Incidents Watch to review and enhance where appropriate the relevant risk management controls, including any applicable customer education efforts.

If there are any questions on the Operational Incidents Watch, please contact Parry Tang on 2878-1524 or Alex Lee on 2878-1484.

Yours faithfully,

Brian Lee
Acting Executive Director (Banking Supervision)

Encl

55th Floor, Two International Finance Centre,
8 Finance Street, Central, Hong Kong
Website: www.hkma.gov.hk

香港中環金融街8號國際金融中心2期55樓
網址：www.hkma.gov.hk

Operational Incidents Watch

Issue No. 2
25 February 2015

Operational Incidents Watch is a periodic newsletter published by the Banking Supervision Department of the Hong Kong Monetary Authority (HKMA). It summarises the major lessons learnt from selected operational incidents[1] that have happened in the banking industry and led to impact on relevant customers or material financial losses of the authorized institutions (AIs) concerned. It aims at facilitating AIs and the members of the public in Hong Kong to stay alert and to take appropriate measures to prevent similar incidents from happening to them.

In this newsletter, the modus operandi or the factors and key control loopholes leading to three types of operational incidents are summarised: (i) misappropriation of an AI's money by a staff member; (ii) loss of certificates of financial instruments pledged for credit facilities; and (iii) belongings stored in a safe deposit box were accessed by another customer.

Misappropriation of an AI's money by a staff member

The incident involved the use of fictitious and unauthorized transactions by an AI's back-office officer, attributed to certain internal control deficiencies including the common practice of sharing user IDs and passwords among staff and inadequate monitoring of suspense accounts.

Modus operandi / factors leading to the incident

The officer, who was senior in the AI's back-office operations, was triggered to consider committing a fraud due to concern of a layoff after a demotion. At the time of the fraud, it was a common practice among staff in the function to share their user IDs and passwords so as to speed up workflows when staff members were on leave or were busy with other activities.

[1] Due to sensitivity considerations, certain details of the relevant operational incidents have been concealed.

The officer firstly created fictitious back-dated money market transactions in the AI's system, where the maker-checker controls were circumvented by using the shared user IDs and passwords. As the fictitious transactions were back-dated, the daily reconciliation checks did not initially uncover those transactions. Then, part of the "interest expense" incurred in the fictitious transactions was transferred into a series of different suspense accounts (including unusual suspense accounts) and a Nostro account of the AI. Thereafter, the officer utilized other colleagues' user IDs and passwords to execute instructions to effect payments from the Nostro account to his own account maintained in another AI.

The fraud remained undetected for a few months until an enquiry was triggered by the bigger difference between the amount of "interest expense" and "interest income" arising from the fictitious transactions noted by the AI's finance function.

Control loopholes and lessons learnt

i. The AI failed to prevent and detect the common practice of sharing of user IDs and passwords among the staff in the back-office function. The consequences (e.g. disciplinary actions) had not been clearly communicated to its staff. In addition, the approval controls of back-dated transactions were insufficient. The AI also did not adequately monitor the opening of suspense accounts and related transactions, and did not sufficiently reconcile interest income against interest expenses.

ii. Besides, the "three lines of defence" framework of the AI was not robust enough in managing the relevant operational risks, given that the relevant control deficiencies had remained unchallenged by both the second line of defence (e.g. operational risk management) and third lines of defence (e.g. internal audit) over a period of time.

Loss of certificates of financial instruments pledged for credit facilities

It was suspected that the certificates of some financial instruments pledged for credit facilities might have been taken away by a credit administration officer, who kept the key to the vault (where the certificates of the pledged instruments were stored), after being asked to leave the AI.

Modus operandi / factors leading to the incident

While a Human Resources (HR) colleague was supposed to accompany the credit administration officer to tidy up his belongings before leaving the AI's premises, the HR colleague left the credit administration officer alone for a short period of time due to other ad-hoc matters. According to the CCTV's footage, the credit administration officer then entered into a storage room where the vault was located with another colleague for work hand-over. After asking his colleague to leave the storage room, the credit administration officer managed to stay in the storage room alone for some time, in violation of the policy that no single person was allowed to access the storage room and the vault. Subsequently, it was also unveiled that the supervisor of the credit administration officer had failed to collect the key of the vault from the officer earlier on that day. After realizing the loss of the certificates of the pledged instruments, the AI reported the incident to the Police and took other actions to safeguard the AI's interest.

Control loopholes and lessons learnt

i. The AI failed to exercise sufficient monitoring and restrictions to ensure that the concerned credit administration officer did not have access to sensitive documents and information once he was asked to leave the AI. In particular, the AI did not require the concerned officer to surrender the key to the vault to his supervisor in a timely manner.

ii. Staff did not follow the AI's internal policy to strictly maintain proper physical access control to the storage room where the vault was located. For

instance, no control register was established and there was inadequate restriction on staff's access to the storage room. There was also insufficient awareness among the relevant staff about the policy that no single person should access the storage room and the vault.

Belongings stored in a safe deposit box were accessed by another customer

When a customer suspected that the inner cylinder of his safe deposit box was storing the belongings of another person after an AI broke open the box, the customer was still allowed to check the belongings in the cylinder without the presence of the AI staff, even though the items contained in that cyclinder in fact belonged to another customer who rented an nearby safe deposit box.

Modus operandi / factors leading to the incident

The two customers (A and B) rented deposit boxes that were located close to each other. On one occasion, they went to the AI and accessed their deposit boxes at the same time but each of them inadvertently inserted the inner cylinder into another's safe deposit box and incorrectly took away the associated key.

When A was unable to unlock his safe deposit box later, he agreed with the AI to break open the box with the help of a locksmith. Once the inner cylinder was taken from the safe deposit box, A indicated that the items in the cylinder probably did not belong to him because it was much heavier than he expected. However, the AI staff failed to advise A to check the content in the inner cylinder with the presence of the AI staff. Instead, A was allowed to take the inner cylinder into the private room of the vault for checking. After A's confirmation that the items did not belong to him, the AI staff allowed the locksmith to use the master key and A's own key to try to unlock other nearby deposit boxes in order to find A's inner cylinder. B's deposit box was then unlocked successfully by the locksmith and A was, after his confirmation on the belongings inside, allowed to take the inner cylinder into the private room for checking. A was also allowed to take away

some belongings inside after some verification of the items, before the inner cylinder was inserted back to B's deposit box for locking.

Subsequently, the AI arranged the two customers and an independent solicitor to be present at the same time to re-open the concerned safe deposit boxes. After checking the belongings inside the correct inner cylinder, B claimed that some of his belongings could not be located and the case was then reported to the Police.

Control loopholes and lessons learnt

i. The AI did not properly handle the incident. For instance, the relevant AI staff failed to advise A against conducting checking on the contents of the inner cylinders without the presence of the AI staff. Moreover, the AI staff failed to seek the consent of other customers before allowing the locksmith to open other nearby safe deposit boxes. Besides, the AI staff did not fully follow the relevant internal procedures for handling the situation and the team supervisor failed to stay in the vault all the times during these processes.

ii. The AI did not have established measures in place to handle situations where customers with nearby safe deposit boxes had access to their boxes at the same time, so as to reduce the chance of customers' inadvertent insertion of inner cylinders into wrong safe deposit boxes.