HONG KONG MONETARY AUTHORITY
香港金融管理局

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

30 June 2015

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Operational Incidents Watch

The Hong Kong Monetary Authority published today the enclosed third 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 Mr Parry Tang at 2878-1524 or Ms Debora Chan at 2878-1593.

Yours faithfully,

Henry Cheng
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. 3
30 June 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 customers' funds in dormant accounts by a staff member; (ii) fabrication of loan documents and unauthorized modification of remittance instructions; and (iii) deviation from pricing basis agreed with clients.

Misappropriation of customers' funds in dormant accounts by a staff member

The incident involved fraudulent funds transfers from dormant customer accounts in an AI, which were made possible by a back-office team leader via misleading his team members or using their system login credentials.

Modus operandi / factors leading to the incident

The team leader was in charge of a back-office team which handled balance transfer and account closure of dormant customer accounts. The team leader managed to conduct unauthorized funds transfers from some dormant accounts to the bank accounts of certain companies maintained in the AI. While the AI implemented maker-checker dual controls over funds transfers from dormant accounts, the team leader circumvented the maker-checker controls by misleading

[1] Due to sensitivity considerations, certain details of the relevant operational incidents were omitted.

his team members to effect the concerned funds transfers or use other team members' system IDs and passwords to effect the transfers (which might involve sharing of passwords, or failure of individual team members to promptly logout the system).

Control loopholes and lessons learnt

i. Workflow of the back-office team had not been subject to adequate fraud risk evaluation. In particular, excessive authority had been delegated to the team leader. There was also a lack of proper reconciliation on the funds transfers between dormant accounts and the AI's ledger account. Moreover, monitoring of large-value funds transfers from dormant accounts was insufficient.

ii. Fraud awareness and risk culture of the team members were also weak. For instance, some team members were asked by the team leader to conduct the suspicious funds transfers without questioning their validity, whereas others might have failed to logout their systems in a timely manner or even shared their login credentials with the team leader.

Fabrication of loan documents and unauthorized modification of remittance instructions

The incident involved an AI's staff member fabricating certain loan documents and modifying the relevant remittance instructions so as to obtain approval for loan disbursement and to subsequently remit the proceeds to her personal bank account.

Modus operandi / factors leading to the incident

A clerk of the AI's loan processing team was responsible for collecting customers' loan applications and processing loan disbursement. At the time of the incident, the clerk experienced financial stresses and she fabricated certain loan documents by referring to old documents or modifying genuine documents (e.g. falsifying a higher loan amount) and then obtained management's approval for disbursement of

the loan proceeds related to fake loan applications. After the SWIFT remittance instructions for the approved loan disbursement transactions were duly authorized and sent to the correspondent banks for disbursing the loan proceeds to the customers' bank accounts, the clerk created and authorized free format SWIFT messages (e.g. MT199) in the AI's system[2] to amend the remittance instructions so that the loan proceeds were transferred to her bank account. During the process, she also created certain free format SWIFT messages for amending the relevant remittance instructions (e.g. to recall the funds transferred to her bank account) and removed the falsified documents to cover up the incident.

Control loopholes and lessons learnt

i. Checker-maker dual control was not established in the AI's system for the creation, authorization and transmission of free format SWIFT messages.

ii. There was inadequate segregation of duties in the AI's handling of customers' loan applications where the concerned clerk was allowed to collect customers' applications, confirming with the customers the loan details, and creating the records in the system.

iii. Control over the receipt and distribution of inward SWIFT messages was inadequate, and hence a series of SWIFT messages exchanged between the AI and its correspondent banks regarding the amendments of remittance instructions were not routed to the supervisors for attention or review.

iv. The supervisors did not exercise due care in reviewing the loan applications/documents before approving the loan disbursements, especially because there was a shortage of staff during the relevant time. They did not scrutinize the underlying reason for the returned loan proceeds after the clerk sent a free format SWIFT message to a correspondent bank to recall the loan proceeds transferred to her personal account.

[2] In the AI's system, a single user was allowed to create, authorize and transmit free format SWIFT messages.

Deviation from pricing basis agreed with clients

There had been discrepancies between the pricing arrangement agreed with clients and the actual prices applied for conducting and pricing certain financial transactions for a number of years before it was discovered. A similar incident also happened to another AI regarding other financial products offered to its clients.

Modus operandi / factors leading to the incident

In one case, the inconsistency was resulted from the AI applying changes to the pricing basis for certain financial products in its IT system and incorrectly changing the agreed pricing basis for other clients as well. Furthermore, the inconsistency was not uncovered at that time due to a lack of control to ensure that any change in pricing calculation applied to the system followed the terms agreed with the relevant clients. In another case, the original design of the AI's IT system adopted a pricing basis different from the terms agreed with the clients concerned, potentially due to ineffective communications between the relevant business department and the department that designed the IT system. In both cases, the AIs took steps to rectify the inconsistencies in their computer systems and arranged compensations for affected clients. Measures were also implemented to prevent similar incidents from happening again.

Control loopholes and lessons learnt

i. There was insufficient communication among the relevant departments in designing or making changes in the AIs' IT systems.

ii. No comprehensive checking or periodic sample checking had been performed after system change between pricing basis and the terms agreed with clients.