HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref : B1/15C
B9/81C

19 September 2014

The Chief Executive
All Authorized Institutions

Dear Sir / Madam,

Operational Incidents Watch

The Hong Kong Monetary Authority published today the enclosed first issue of the 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 Mr Alex Lee at 2878-1484.

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. 1
19 September 2014

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; (ii) inadequate follow-up of loan drawdown conditions; and (iii) fake cashier's order.

Misappropriation of customers' funds by staff

There were a number of incidents involving misappropriation of customers' funds by AIs' staff, where the major causes were non-adherence to AIs' internal procedures by other staff in verifying customers' transactions, insufficient checks and balances in the relevant operations or inadequate alertness of the customers concerned.

Modus operandi / factors leading to the incident

Certain incidents involved senior front-line staff members who gained trust from some customers and conducted deposits or withdrawals on behalf of the customers over branch counters without the presence of those customers. They lured the customers to directly pass the cash/cheques to them for deposit or sign blank cash withdrawal slips. They even forged the customers' signatures to early uplift customers' fixed deposits. The funds (cash or crossed cheques) received from

[1] Due to sensitivity considerations, certain details of the relevant operational incidents are not summarised.

customers through the above means were, on some occasions, misappropriated by the staff members or actually deposited to other victims' bank accounts[2] so as to cover up the misappropriation.

As most of the affected customers were standalone fixed deposit customers who did not receive regular bank statements, the staff members took steps to prevent the victims from noticing abnormal transactions conducted in their bank accounts. For instance, the staff members provided the customers with forged fixed deposit confirmation slips and withheld the genuine transaction advices (e.g. cash transfer/withdrawal slips) of the customers' bank accounts. Through these tactics and other control lapses (see below), the staff members managed to misappropriate the affected customers' money without being detected for a period of time.

Separately, a team leader who was supposed to monitor the process of counting cash received from customers was also permitted to participate in cash counting. As the AI concerned did not strictly require more than one staff at all times during the cash counting process in the absence of customers, the team leader was able to steal money when all the cash counting staff were away for a while during the cash counting process.

Control loopholes and lessons learnt

i. The branch tellers did not follow the established procedures to verify cash withdrawals or early uplifting of fixed deposits with the relevant customers but instead relied solely on senior front-line staff members' confirmations.

ii. No report monitoring early uplifting of fixed deposits and overridden cheque deposits was produced or reviewed, and no regular balance confirmations with stand-alone fixed deposit customers had been performed.

iii. Job rotation plan and block leave requirements for front-line staff were absent or were not implemented.

[2] The staff members deposited crossed cheques into other victims' accounts by exercising their overriding authorities.

iv. The affected customers did not check their transactions with branch tellers directly or obtain their deposit/withdrawal confirmation slips directly from branch tellers.

v. The records of CCTV on cash counting were not regularly reviewed, and there was inadequate safekeeping of cash being counted when the counting process was suspended (e.g., due to unavailability of cash counting staff).

Inadequate follow-up of loan drawdown conditions

Due to inadequate follow-up and monitoring of loan drawdown conditions and other control deficiencies, material financial loss arising from an overdue equipment financing facility could not be readily recovered by an AI through possession and re-sale of the financed equipment.

Modus operandi / factors leading to the incident

In an equipment finance facility granted by an AI to a borrower, one of the drawdown conditions specified that the equipment should be delivered to a designated destination upon loan disbursement and a physical inspection of the equipment should be arranged shortly after the loan disbursement. However, the marketing officer did not instruct the AI's agent to conduct the equipment inspection until several months after the deadline. After the inspection was finally performed, the agent informed the loan processing unit that the equipment had not been shipped due to delay in custom clearance. The loan processing unit then requested the marketing officer to follow up the matter, without escalating the matter to the business line management or credit risk management function.

The discrepancies in equipment inspection and delivery were not noticed by the AI's management in a timely manner, due to the above-mentioned failure in escalation of the issues to the management and other control deficiencies (see below). The management was aware of these discrepancies only weeks after the

loan became delinquent several months after the loan disbursement. It was also unveiled that the equipment was delivered by the suppliers to another destination as instructed by the borrower, shortly after the loan became overdue.

Although the AI then instituted relevant proceedings to repossess the financed equipment and against the borrower, the shipment of the equipment could have been withheld and the financial loss could have been substantially recovered from possession and re-sale of the equipment if the management had been promptly notified of the discrepancies identified.

Control loopholes and lessons learnt

i. There was an insufficient segregation of duties between marketing officers and the loan processing unit, where the loan processing unit played a passive role in following up the loan drawdown conditions.

ii. The alertness of loan processing unit was also inadequate as reflected by the fact that the loan processing staff did not promptly escalate the major discrepancies in equipment inspection and delivery to the credit risk management function or business line management.

iii. Monitoring and reporting of important outstanding items for loan operations (e.g., equipment inspection) were ineffective. For instance, the relevant MIS report removed outstanding items on equipment inspection from the report or did not highlight those items so long as an instruction for equipment inspection had been placed, even if inspection had not been performed.

Counterfeit cashier's order

The event was related to inadequate caution exercised by an AI's staff during the verification of a fake cashier's order received by the AI, resulting in material financial loss.

Modus operandi / factors leading to the incident

The AI issued a cashier's order, on behalf of a corporate customer, in favour of a new overseas supplier of the customer. Upon request, the customer sent via email a coloured copy of the cashier's order to the supplier as a proof of funds. The business deal was later cancelled and the customer then informed the AI to cancel the cashier's order accordingly. However, the AI found that the cashier's order had been cleared several weeks ago and the fraud proceeds had already been remitted out shortly after the cashier's order was paid in.

Control loophole and lessons learnt

i. The customer should have been more cautious before sending the coloured copy of the cashier's order to the new supplier. For instance, the customer should have sent only a "greyscale" or masked copy of the cashier's order, or used other means as a proof of funds, rather than giving the supplier a coloured softcopy of the cashier's order via email, which could be intercepted during or after the transmission. The customer's cancellation of the cashier's order could also have taken place earlier.

ii. AI's relevant staff did not exercise sufficient care in verifying the cashier's order during the clearing process, although the cashier's order bore a few apparent irregularities on its appearance.