Issue No. 4
30 November 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 or 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 two operational incidents are summarised: (i) use of fraudulent documents and information for obtaining factoring financing; and (ii) unauthorised access to an AI's premises by a staff member during her garden leave period.

Use of fraudulent documents and information for obtaining factoring financing

An AI suffered from a material fraud loss in the provision of factoring financing to borrowers due to inadequate controls and verification for detecting the fraudulent documents and information provided by the borrowers.

Modus operandi / factors leading to the incident

The AI granted trade finance facilities including factoring and export financing to a couple of borrowers. When the borrowers started utilising the factoring limits, the AI initially conducted detailed reviews of the related transaction documents (e.g. the sales invoices and shipping documents) submitted by the borrowers and sent debt confirmations to the approved debtors to verify the genuineness of the underlying transactions. However, after several transactions, the AI no longer

[1] Due to sensitivity considerations, the incidents mentioned in this newsletter could be prepared on the basis of synthesis of multiple incidents or certain details of the relevant operational incidents might have been omitted.

conducted adequate reviews of the transaction documents submitted by the borrowers. Besides, the AI did not perform sufficient checking of the company information of new debtors added to the approved list and the borrowers' requests for changing the contact information of certain approved debtors. For instance, the e-mail addresses (even with private e-mail domain) or the identities of the contact persons of a new debtor provided by the borrowers were not duly verified through independent sources. By exploiting these loopholes, the borrowers were able to obtain factoring financing from the AI by providing fictitious contact information of the approved debtors and producing bogus sales invoices and shipping documents in the subsequent transactions.

Control loopholes and lessons learnt

i. There was a lack of well-established on-going verification of the transaction documents provided by the borrowers. The AI set an inappropriate level of threshold for checking the bills of lading and it mainly relied on debt confirmations sent to the borrowers' approved debtors, via the contact details provided by the borrowers, to ascertain the genuineness of the underlying transactions between the borrowers and their debtors. Subsequent investigation of the case unveiled that there were substantial mismatches between the information stated on the bills of lading submitted by the borrowers and the records maintained by those independent service providers of shipping information (e.g. the International Maritime Bureau and Sea Searcher). Those mismatches had not been detected earlier because the sizes of those underlying trade transactions were all individually below the checking threshold at the relevant time, while the AI did not have a checking threshold that referred to the aggregate utilization of the factoring limits.

ii. The contact information of the approved debtors (e.g. e-mail and business addresses, phone numbers, etc.) provided by the borrowers were not adequately verified by the AI's relevant staff members through reliable independent sources. In addition, the responsibility of verifying the company information of approved debtors provided by borrowers had not been clearly defined among the relationship management team, the factoring credit team and the factoring operations team of the AI. As a result, official company searches and contact

information for some approved debtors were either omitted or not promptly verified. Even when the monthly statements of some approved debtors were returned due to invalid addresses, the factoring operations team did not promptly ask the factoring credit team to verify the debtors' addresses, thereby resulting in delay in detection of the suspicious activities.

iii. The fraud loss could have been reduced if a "probation period" had been imposed on those newly approved debtors with limited verifiable particulars so that the related factoring financing would not be made available to the borrowers until the AI had received payments from those new debtors.

Unauthorised access to an AI's premises by a staff member during her garden leave period

The incident involved a staff member of an AI entering the AI's premises and printing out confidential information during her garden leave period without prior consent.

Modus operandi / factors leading to the incident

The staff member, who was given an official notice of redundancy by the AI, was placed on garden leave prior to her termination of employment. However, the staff member was not required to surrender her building access card and no formal notification was given to her regarding the restrictions that, among others, she could not enter the AI's premises without prior consent during the leave period. Given that the staff member was instructed by her manager to complete certain handover tasks prior to the start of the garden leave, she returned to the AI during the leave period. Having noted that her access to the AI's office area was denied, she requested the AI's Office Administration team to reactivate her access on the ground that she needed to complete the handover work. The Office Administration team then granted her a one-day temporary access to the AI's office area without consulting the Human Resources or the manager of the staff member. Further, the staff member continued to gain access to the AI's office area after office hours on the next few days by only showing her deactivated building access card and

explaining to the building security guards that the access card was not functioning. The AI subsequently picked up these irregularities and then conducted a review of the staff member's activities. Whilst the review found that the staff member printed some confidential documents from the AI's system and took them away from the AI's premises, she explained that the information was only used for completing the handover work. She then returned the hardcopies of the documents to the AI and signed an undertaking that she had not made copies or disseminated the information to third parties.

Control loopholes and lessons learnt

i. There were inadequate process and controls over staff who were placed on leave pending termination of employment, where (i) formal instruction had not been given to the staff member as well as the manager on their responsibilities and obligations during the garden leave period, leading to a misunderstanding by the staff member that she was still allowed to access the AI's premises and IT systems in order to complete the handover work; and (ii) the manager failed to complete the AI's procedures for handling exiting employees to collect the building access card from the staff member and remove her IT system access rights prior to the commencement of the garden leave.

ii. The Office Administration team had not adhered to the AI's physical access authorisation procedures. Appropriate parties of the AI had not been duly consulted before the temporary access to the AI's premises was granted to the staff member.

iii. The building security guards had failed to verify the identities of the staff member and prohibit her access to the AI's premises.