Early Signals of Fraud in Banking Sector

(Revised 2018 Edition)

Digital Accounting and Assurance Board
The Institute of Chartered Accountants of India
(*Set up by an Act of Parliament*)
New Delhi

Revised Edition	:	May, 2018
Committee / Department	:	Digital Accounting and Assurance Board
E-mail	:	gdaab@icai.in
Website	:	www.icai.org; http://pqc.icai.org
Price	:	Rs.400
ISBN No	:	978-81-8441-896-5
Published by	:	Publication Department on behalf of The Institute of Chartered Accountants of India, ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi-110002
Printed by	:	Sahitya Bhawan Publications, Hospital Road, Agra-282003 May/2018/1000 Copies

Foreword

Banking sector has grown by leaps and bound in last few years, and this has also increased the need for more governance, accountability and transparency. The pace of changes puts great challenges for banks to grapple with multiple fraud related challenges, and to develop comprehensive fraud risk management controls that will help in prevention as well as detection of fraud as soon as they occur. E-banking, internet banking and internet fraud are the top fraud risks that are currently posing highest concern for the banks.

Chartered accountants as a new age professional, are making the most out of the opportunities technology offers, through data analytics tools and new skill sets, for combating the risks in banking fraud landscape. With a view to provide comprehensive guidance in this area, Digital Accounting and Assurance Board of ICAI (erstwhile Committee on Information Technology) had released "Early Signals of Fraud in Banking Sector" in 2017. This publication has now been updated to include fraud risks involving information technology covering Core Banking Solutions (CBS), Digital Payment System, Internet Banking, as well as use of Artificial Intelligence in fraud detection. This updated publication provides compilation of various early warning signals thereby enabling members to get cautious, and also provides focus areas to banks on strengthening fraud risk management strategy.

I complement CA. Atul Kumar Gupta, Chairman, DAAB, CA. Manu Agrawal, Vice Chairman, DAAB, and other members of the Board for bringing out revised and updated edition of this publication, which would help our members in discharging their professional duties efficiently.

Place: New Delhi **CA. Naveen N. D. Gupta**

Date: May 18, 2018 President, ICAI

Preface

Banking sector is like an engine that drives the operations in the financial sector, money markets and growth of an economy. As complexity of banking sector has increased over the years, the need for culture of eternal vigilance, strong internal control system and compliance for developing fraud free eco system has increased exponentially. Banks need greater commitment and sensitivity to mitigating and managing fraud risk by developing robust fraud risk identification, control, and mitigation framework. Further, as technology evolves from being an enabler to being at the core of the banking operations, security related issues need to be addressed comprehensively.

Chartered accountants play a crucial role in fraud risk management framework by evaluating the preventive and detective controls in the banks and ensuring that preventive controls are working as intended. With a view to equip members in this critical area, Digital Accounting and Assurance Board (erstwhile Committee on Information Technology)of ICAI has brought out revised and updated publication "Early Signals of Fraud in Banking Sector" which would assist them to be instrumental in timely detecting fraud and also suggesting controls for prevention. Apart from incorporating impact of revised circular, this revised edition also includes fraud risks involving information technology covering Core Banking Solutions (CBS), Digital Payment System, Internet Banking. Further, a new section has also been added on use of artificial intelligence in fraud detection. Integration of IT security and fraud management capabilities is required to address the increasingly technical nature of fraud attacks. In this publication, fraud risks have been classified in seven categories – operations of account, concealment or falsification of documents, diversion of funds, issues in primary/ collateral security, inter-group/ concentration of transactions, regulatory concerns, and other signals.

At this juncture, we wish to place on record my sincere thanks to CA. Srinivas Y. Joshi, CA. G.N. Sampath, CA. Kuntal Shah, CA. Dhananjay Gokhale, CA. Gautam Shah, CA. Ketan Saiya, CA. Manish Sampat, CA. Nilesh Joshi, CA. Niranjan Joshi, CA. Sandeep Welling, CA. Sanjay Khemani, CA. Vikas Kumar, CA. Abhijit Sanzigiri, Dr. Manish Srivastava, for taking time out of their pressing preoccupations and contributing in preparation of draft of this

important publication of the Board.

We would like to express our gratitude to CA. Naveen N.D. Gupta, President ICAI and, CA. Prafulla Premsukh Chhajed, Vice President, ICAI for their continuous support and encouragement to the initiatives of the Board. We also wish to place on record our gratitude for the all Board members, co-opted members and special invitees for providing their invaluable guidance and support to various initiatives of the Board. We also wish to express sincere appreciation for CA. Jyoti Singh, Secretary, DAAB, and CA. Amit Gupta, Asst. Secretary, DAAB, for their efforts in bring out this revised publication.

We are sure that the members and other interested readers would find this revised publication immensely useful.

CA. Atul Kumar Gupta
Chairman, DAAB

CA. Manu Agrawal
Vice-Chairman, DAAB

Place: New Delhi

Date: May 23, 2018

Contents

Introduction

Master Directions on Frauds – Classification and Reporting by commercial banks and select FIs, dated 1st July 2016 (updated as on July 03, 2017)

Reserve Bank of India, as a regulator of Banking Industry in India, has issued several Master Circulars and Master Directions which guide the banks on various aspects of banking. One such important guidance given by RBI is in case of Frauds in Banks. The Master Directions on Frauds dated. 1st July 2016 (updated as on July 03, 2017) are issued to provide a framework regarding detection and timely reporting of frauds by banks to the regulator. It also requires banks to take timely action against fraudsters as well as the staff involved. The directions require banks to put in place measures by way of appropriate procedures and internal checks to prevent such occurrences in future.

RBI has not defined the meaning of term "Fraud" in its Master Directions. However, RBI working group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds has defined Fraud as "A deliberate act of omission or commission, by any person, carried out in the course of a Banking Transactions or in the Books of Accounts maintained manually or under Computer System in Banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the Bank."

There are two types of frauds possible in Banking Industry –

(a) Frauds in Banks

(b) Frauds on Banks

Frauds in Banks would include- Cash lending during working hours, Missing notes in bundles, Use of same note bundles by two branches, Posting in wrong accounts, Misuse of sensitive stationery, etc. These frauds are made by Bank's Staff.

Frauds on Banks would include – Technology related Frauds, Deposit related Frauds, Advances Portfolio Frauds, etc.

Technology related Frauds– Greater Technology integration in Banks makes customer use platforms like Mobile, Internet and Social Media for enhancement of efficiency and cutting of costs. Online banking and transfers

by NEFT and RTGS, use of ATM/Debit/Credit Card have become order of the day.

The fraudsters employ hostile software programs or malware attacks, phishing (mails), vishing (voice-mail), SMSishing (Text messages), whaling (Targeted phishing on high net worth individuals), Card duplication Techniques apart from stealing confidential data to perpetrate Frauds.

Deposit related Frauds – Lack of compliance with KYC Guidelines, misuse of inoperative accounts, Non-reconciliation of Suspense and Sundry Accounts and lack of control over transactions, in these accounts, result in frauds.

Advances Portfolio Frauds – Majority of credit related frauds are on account of deficient appraisal system, Poor post- disbursement supervision and inadequate follow-up. Most of the frauds relating to advances come to light only during the recovery process initiated after the accounts have been classified as NPA. Fabricated/fudged Financial Statements, inflated security valuation report, defective search report for title deeds of mortgaged property are commonly discovered.

The most effective way of preventing frauds in loan accounts is for banks to have a robust appraisal and an effective credit monitoring mechanism during the entire life-cycle of the loan account. Any weakness that may have escaped attention at the appraisal stage can often be mitigated, in case the post disbursement monitoring remains effective. In order to strengthen the monitoring processes, inclusion of the following checks during the different stages of the loan life-cycle should be carried out:

(a) Pre-sanction: As part of the credit process, the checks being applied during the stage of pre-sanction may consist of the bank collecting independent information and market intelligence on the potential borrowers from the public domain on their track record, involvement in legal disputes, raids conducted on their businesses, if any, validation of submitted information/data from other sources like the ROC, scanning the defaulters list of RBI/other Government agencies, etc., which could be used as an input by the sanctioning authority.

(b) Disbursement: Checks during the disbursement stage, shall, among others, focus on the adherence to the terms and conditions of sanction, rationale for allowing dilution of these terms and conditions, level at which such dilutions were allowed, etc. The dilutions should strictly conform to the broad framework laid down by the Board in this regard. As a matter of good practice,

the sanctioning authority may specify certain terms and conditions as 'core' which should not be diluted.

(c) Annual review: While the continuous monitoring of an account through the tracking of EWS is important, banks also need to be vigilant from the fraud perspective at the time of annual review of accounts. Among other things, the aspects of diversion of funds in an account, adequacy of stock, stress in group accounts, etc., should also be considered at the time of review. Besides, the Bank should track market developments relating to the major clients of the bank. This would involve collecting information from the grapevine, following up stock market movements, subscribing to a press clipping service and monitoring databases on a continuous basis.

RBI Master Directions on Frauds dated. 1st July 2016 lists out 42 Early Warning Signals of Frauds. They can be classified into following categories -

1. Operations of Account - Bouncing of high value of cheques, frequent invocation of BGs and devolvement of LCs, frequent request for general purpose loans, frequent adhoc sanctions, etc.
2. Concealment or Falsification of documents – Substantial increase in unbilled revenue year after year, poor disclosure of materially adverse information, material discrepancies in annual report, etc.
3. Diversion of Funds – Non- routing of sales proceeds through consortium banks, high value RTGS payment to unrelated parties, increase in borrowings despite huge cash equivalents in the balance sheets, etc.
4. Issues in Primary/Collateral Security – Critical issues highlighted in the stock audit report, significant movements in inventory and receivables disproportionately differing vis-à-vis change in the turnover, etc.
5. Inter-Group/Concentration of Transactions – Funds coming from other banks to liquidate the outstanding loan amount, substantial related party transactions with inter- connected companies and large outstanding from such companies, etc.
6. Regulatory Concerns – Default in undisputed payment to the statutory bodies, raid by Tax Authorities.
7. Others - Resignation of key personnel and frequent changes in management, significant reduction in stake of promoters, etc.

These Early Warning Signals are red flags, which need immediate attention and action by the Management of the Banks. The classification given above is broad, and various instances can overlap each other.

Therefore, it should be remembered that –

(a) No one signal can be seen in isolation

(b) Existence of such signals does not necessarily mean that there is a fraud

(c) In case of fraud, several signals would appear together

Bank should build processes and control for prevention and timely detection of frauds. Such controls can be internal or external, manual or information technology- based. Timely scrutiny of the data received by the management having appropriate knowledge can only be the effective check on frauds.

Various Early Warning Signals and the responses of the Bank Management and Auditors to such signals, as well as the use of Information Technology by Fraudsters in committing frauds have been given in detail in subsequent write-ups.

Frauds Risks involving Information Technology (IT)

Information Technology (IT) plays a significant role in development of Digital banking to make the banking fast, effective and efficient. Use of IT in banking system made banking more customer oriented, quality driven and easy to use by both bank and customer. Various initiatives has been taken by the banks to converge their self from traditional banking to Digital banking. The initiatives took by the banks are as follows-

1. Core Banking Systems (CBS)
2. Digital Payment System
3. Credit / Debit Cards
4. ATMs/ POS Terminals/CDMs
5. Internet Banking like NEFT/RTGS
6. Mobile Banking
7. Branchless Banking
8. Digital Wallet

These initiatives were effectively adopted by the customer and has increased the profitability and customer base for the banks. The initiatives has also increased the productivity as well as ease of banking for the customer.

Like other technologies, IT is also not an exceptional, and may prone to trick by the humans having advance skills to exploit. There are various ways by which these initiatives for the digital baking can be exploit by the hacker or

thief or an anti-social element. The following are one of the most common ways in which exploitation of IT is being done on the most popular initiatives-

1. **Fraud Risk on CBS:** When the letter of understanding (LOU) issued, message for the credit transfer conveyed to the overseas banks through SWIFT (Society for Worldwide Interbank Financial Telecommunication) System by the sending bank and this message through SWIFT is termed as sending bank's consent and guarantee to the overseas bank.

   The sending bank official must log into its CBS system to route the transaction on SWIFT. The fraud on CBS occurs when SWIFT is not integrated with CBS and a perpetrator can easily sends LOUs to overseas bank simply bypassing the CBS.

2. **Fraud Risk on Digital Payment System:** Digital payment system spread across globe due to its scalability and acceptability by all class of users. Handling of account by a user either through online or through mobile is increasing day by day and hence they are the common target for the perpetrator. The perpetrator may deploy different techniques to make fraud happen. Some techniques are explained as follows-

   2.1 Phishing: Perpetrator use to send emails to lure users, that he has won the lottery or some money needs to be deposited in his account and then requesting user to provide the details of his bank account.

   2.2 Device Compromise: Device through which bank customer is operating his account either through online or through mobile usually prone to be compromised by perpetrator for execution of the fraud. Compromising the Operating system of the smart phone or any other status change like firewall setting etc. may lead to fraud.

   2.3 Man in the Middle Attack: Perpetrator, in this case, altering the communication between the two legitimate parties and execute the fraud. The legitimate parties think that they are communicating with one another but in real scenario their communication is received and altered by the perpetrator.