SOUTH INDIAN Bank
Experience Next Generation Banking

STUDENTS'
ECONOMIC FORUM

A monthly publication from South Indian Bank

To kindle interest in economic affairs...
To empower the student community...

www.southindianbank.com
OPEN ACCESS Student's corner
ho2099@sib.co.in

SEPTEMBER 2018

Theme 322

"FRAUD RISK MANAGEMENT IN BANKS"

27th Year of Publication

SIB MSME Loan

No matter whether your enterprise is micro, small or medium, we give wings to your entrepreneurial ambition.

Customised loan product | Competitive interest rates | Low processing fee | Hassle-free procedure | Quick disbursal

SOUTH INDIAN Bank

Experience Next Generation Banking

Toll Free (India): 1800-843-1800, 1800-425-1809 (BSNL), Email: sibcorporate@sib.co.in | CIN : L65191KL1929PLC001017

www.southindianbank.com | /thesouthindianbank

Theme No: 322:**"Fraud Risk Management in Banks**"

A well informed customer will make the policy makers as well as organizations which produce goods and render services more responsive to the customer needs. This will also result in healthy competition among organizations and improve the quality of its products.

The "SIB Students' Economic forum" is designed to kindle interest in the minds of younger generation. We highlight one theme in every monthly meeting of the "Forum". This month the topic for discussion is "Fraud Risk Management in Banks".

In recent years, frauds reported (For more than Rs. 1 lakh) in the Indian banking sector show an increasing trend both in terms of number and quantum. Indian banks reported a total loss of about Rs 70,000 crore due to frauds during the last three fiscals up to March 2018. The extent of loss in fraud cases reported by scheduled commercial banks (SCBs) for the last three years is given below:

(Rs. in Crore)

Sl. No	Particulars	2015-16	2016-17	2017-18
1	Fraud Loss	16,409	16,652	36,694

While the bulk of banking frauds was loan-related, it is observed that there has been a significant jump in card and internet banking related frauds during 2017-18.

A total of 972 such incidents were reported in 2017-18, roughly three per day. The banking sector lost a total of Rs 168.74 crore to organised crimes directed at ATMs in the past three years. With a lot of essential financial services shifting to the digital space, the number of frauds targeting online transactions has also increased. In 2017-18, a total of 911 frauds were committed using debit and credit cards. The sum total of money that went into the wrong hands stands at Rs 65.26 crore.

The Reserve Bank of India has changed the norms to reduce the liability of customers with regard to card related frauds. The liability will be shared by banks and customers depending on the circumstances under which the fraud took place. Customers are exempted from liability if the fraud has happened due to negligence of the bank or a third-party breach where the liability is not on the bank or the customer, but on the system. On the other hand, customers will have to bear the loss if fraud has occurred due to negligence on their part. In such cases, customers are liable for losses accrued before they report the same to the bank.

What is Fraud and the different types of fraud?

The term 'fraud' commonly includes activities such as theft, corruption, conspiracy, embezzlement, money laundering, bribery and extortion.

Fraud can result from many varied relationships between offenders and victims. Examples of fraud include:

a. Crimes by individuals against consumers e.g. misrepresentation of the quality of goods.
b. Employee fraud against employers, e.g. payroll fraud, falsifying expense claims, thefts of cash, assets or intellectual property (IP), false accounting.
c. Crimes by businesses against investors e.g. financial statement fraud.
d. Crimes against financial institutions, e.g. using lost and stolen credit cards, cheque frauds.
e. e-crime by people using computers and technology to commit crimes, e.g. phishing, spamming, copyright crimes, hacking.

Briefly describe the framework for dealing with Loan frauds in banks.

i. Identification of Red Flagged Account (RFA) - A RFA is one where a suspicion of fraudulent activity is thrown up by the presence of one or more Early Warning Signals (EWS). These signals in a loan account should immediately put the bank on alert regarding a weakness or wrong doing which may ultimately turn out to be fraudulent.

A few Early Warning Signals are listed below, in order to classify an account as Red Flagged Account.

a. Financing the unit far away from the branch.
b. Substantial increase in unbilled revenue year after year.
c. Disproportionate increase in other current assets.
d. Substantial related party transactions.
e. Not routing of sales proceeds through bank.

ii. Early Detection and Reporting: 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.
    a. Pre - Sanction: Bank collecting independent information and market intelligence on the potential borrowers and validation of submitted information/data from other sources like the ROC, gleaning from the defaulters list of RBI/other Government agencies, etc.
    b. Disbursement: The disbursement stage is focused on the adherence to the terms and conditions of sanction.

iii. Role of Auditors: Auditors coming across the instances of fraudulent transactions in the account should immediately bring it to the notice of the top management and Audit Committee of the Board (ACB) for appropriate action.

iv. Prompt Reporting: In case of accounts classified as 'fraud', banks are required to make provisions to the full extent immediately, irrespective of the value of security. However, in case a bank is unable to make the entire provision in one go, it can spread it to four quarters provided there is no delay in reporting.

In a nutshell, the points to be kept in mind at the time of lending are:
a. Follow the 5 'Cs" of CREDIT - Capacity, Capital, Collateral, Conditions and Character.
b. Use extensively the 3 Cs – CFR (Central Fraud Registry), CRILC and Credit Bureaus like CIBIL.

What are the measures taken for combating fraud in the digital front?
Technology adoption by banks has increased manifold in the recent years and if a bank is not present in the digital space it would be impossible for it to compete in the market. As technology evolves from being an enabler and differentiator to being at the core of the banks' operations, associated issues of security need to be addressed comprehensively.

There is an increasing trend in incidents pertaining to theft of personal information, abuse of ATMs and Distributed Denial of Service (DDoS) attacks on various banks. Risk.net published an article on the Top 10 Operational Risks for 2017 and indicated Cyber Risk as the top most risk in the minds of Chief Risk Officers.

Banks have taken initiative in bringing up the FRM (Fraud Risk Management Solution) in the digital platform of the respective products and services offered.

Fraud Risk Management solution is an additional authentication which is added into the system to calculate the risk profile of the user. The system will understand the transaction and usage pattern of the user and identify the risk associated in performing the transaction/activity based on the risk profile of the user and the transaction is challenged with second factor authentication.

In other words the system will Allow / Challenge / Deny the transaction of the user based on the risk associated with the transaction.

i. If risk associated with the transaction is low, system will allow the user to perform the transaction. In such cases only PIN will be required to perform the transaction/activity.

ii. If risk associated with the transaction is high, system will challenge the user to answer any one of the already opted security questions. Based on the answer the user will be allowed to perform the transaction.

iii. If risk associated with the transaction is very high, system will deny the user from performing such a transaction and system will automatically intimate the same to FRM cell for analysis.

Apart from the FRM solution, Banks have come up with measures of self locking the account when it's not being used i.e., blocking the transactions through any of the digital channels viz ATM/ Internet Banking / Online Transaction / Mobile Banking which will prevent hacking of the account.

Digital e-lock

With the Digital e-lock on SIB Mirror+ App, you can lock or unlock your account from anywhere, at the touch of a finger. And protect all your digital transactions.

Tap to lock/unlock | Protection for digital transactions against frauds | SIB Mirror+ App can be downloaded from Google Playstore, App Store or Windows Store.

Download it now!

Google play

Download on the App Store

Windows Phone

SOUTH INDIAN Bank

Experience Next Generation Banking

Toll Free (India): 1800-102-9408, 1800-425-1809 (BSNL), Email: sibcorporate@sib.co.in, CIN : L65191KL1929PLC001017

www.southindianbank.com | /thesouthindianbank