FRAUD RISK MANAGEMENT

S.D.N. Perera *CISA, B.Com.,Dip.Bank Mgmt*

1. Introduction

Fraud Risk Management is one of the key components of the Operational Risk Management Program. Fraud is a subject that needs attention not only of the Auditors but also Business Managers and the entire Corporate and the Board of Management inclusive of Board of Directors. This Paper brings about the nature and facts about fraud with more concern for employee frauds. Let us start quoting a section of a paper appeared in the Institute of Internal Auditors Journal "The Truth about Fraud" and then highlight the impact of the largest Corporate Fraud hitherto known i.e. "Enron" is quoted to draw attention to the nature of the risk we are exposed to. One needs to understand the type of frauds and why people commit fraud in order to pursue a Fraud Risk Management Programme. Therefore, in this paper these matters as well as some of the common frauds that can be found in banks are discussed in detail with Risk mitigation measures.

2. The Truth about Fraud

"Fraudulent activity is rampant in today's organizations, and there are many surveys to prove it.In reality, fraud effects all organizations. And the behaviour is not just limited to crooks and con artists – it's a tendency that exists in almost every individual. We may not recognize the extent of fraud around us, because many types of dishonesty are tolerated by society. "

"Fraud is not the exception; it's the norm. When deciding whether to engage in dishonest behaviour, people are often more likely to consider whether they can get away with it rather than whether the behaviour is right or wrong."

"Believing that it's okay to do the "wrong thing," as long as no one gets caught, is the underlying cause of many frauds."

Source : Institute of Internal Auditors, USA – Journals and - website www.theiia.org.

2.1 Enron Episode

"Enron" was a multinational company that specialized in markets, in electricity, natural gas, energy, and other physical commodities. Enron initiated the wholesale natural gas and electricity markets in the United States. It was officially formed in 1985 as a result of the merger of Houston Natural Gas and InterNorth of Omaha, Nebraska. In 2000, Enron reported revenues of $101 billion, making it the seventh largest U.S. company in terms of revenue. In 2000, Enron employed 21,000 employees and operated in over 40 countries.

In October 2001, Enron was suspected of a large financial statement fraud. It appears that Chairman Kenneth Lay, former President Jeffrey Skilling, and former Chief Financial Officer Andrew Fastow, among others, were actively involved in partnerships that helped shield debt from public view and give the impression of rapid profit growth in its stock price, which reached a height of $90 earlier in the year, dropped to less than $1 in a matter of days. Unfortunately, in 2002, Enron was fighting to avoid collapse in one of the biggest corporate failures in U.S. history. Enron was being sued for $25 billion, with new lawsuits being added.

Enron citing accounting errors, had to restate its financial statements, cutting profits for the past three years by about 20 percent or around $586 million. Many of the lawsuits against Enron alleged that executives reaped personal gains from "off-the-book" partnerships, while the energy giant violated basic rules of accounting and ethics. As the accounting discrepancies became public knowledge, Enron investors lost billions of dollars, shattering their retirement plans. New York-based Amalgamated Bank, which lost millions in the fraud, is currently suing 29 top Enron executives. Enron has filed for Chapter II bankruptcy, making it the largest corporation ever to file for bankruptcy. Enron's bankruptcy has now been exceeded in size by WorldCom's bankruptcy. In addition to Enron's internal accounting problems, its auditor, a "Big 5" CPA firm, allegedly instructed employees to destroy documents related to its work on Enron. That accounting firm, Arthur Andersen, has now gone out of business because of its involvement in the Enron Fraud. The magnitude of this alleged fraud has shattered public confidence in America's financial reporting system.

In reacting to the Enron scandal, The American Institute of Certified Public Accountants (AICPA) released the following statement to all AICPA members:

"Our profession enjoys a sacred public trust and for more than one hundred years has served the public interest. Yet, in a short period of time, the stain from Enron's collapse has eroded our most important asset: Public Confidence."

2.2 Seriousness of the Fraud Problem

Enron is an example of a company whose management misrepresented the company and allegedly committed fraud. This is just one of the many types of frauds that are a major problem for businesses throughout the world.

Although most people and even researchers believe that fraud is increasing both in size and frequency, it is very difficult to know for sure. First, it is impossible to know what percentage of fraud perpetrators are caught. Are there perfect frauds that are never discovered, or are all frauds eventually discovered? In addition, many frauds that are discovered are handled quietly within the victim organization and never made public. In many cases, companies merely hide the frauds and quietly terminate or transfer perpetrators rather than make them public.

3. What is fraud?

There are two principal methods of getting something from others illegally: by use of physical force and by trickery. The first type of theft is called *robbery*, and the second type - fraud. Robbery is generally more violent and more traumatic than fraud and attracts more media attention, but losses from fraud far exceed losses from robbery. Fraud always involves deception, confidence, and trickery.

Although there are many definitions of fraud, probably the most common is the following:

"Fraud is a generic term, and embraces all the multifarious means which human ingenuity can devise, which are resorted to by one individual, to get an advantage over another by false representation. No definite and invariable rule can be laid down as a general proposition in defining fraud, as it includes surprise, trickery, cunning and unfair ways by which another is cheated. The only boundaries defining it are those which limit human knavery."

Fraud is deception that includes the following seven elements:

- A representation
- About a material point,
- Which is false,
- And intentionally or recklessly so,
- Which is believed
- And acted upon by the victim
- To the victim's damage

Fraud is different from unintentional errors. If someone mistakenly enters incorrect numbers on a financial statement, it is not fraud, because it was not done with intent or for the purpose of gaining advantage over another through false pretense. But, if someone purposely enters incorrect numbers on a financial statement to trick investors, then it is fraud!

One of the most famous frauds of all time was Charles Ponzi's investment scam. This scam is somewhat similar to a pyramid scheme and that was much in focus in recent past and even now. Ponzi perpetrated a fraud by promising to pay investors unusually high returns. Two interesting things about Ponzi's scheme were that (1) he never made any of the promised investments, but (2) he actually paid the promised returns – at least initially. To make the "investment" look legitimate, Ponzi duped investors into believing he was providing "returns," at least for a while. Thus, early on if someone invested $1,000 in the scam, for example, he paid the promised return of $300 at the end of the year. In reality, the $300 was a refund of part of the original $1,000 investment, which left only $700 in the investment, but it appeared as though the investor was earning a 30 percent return. Thrilled with the high "returns," investors poured more money into the investment and spread the word about this hot investment. As a result, the scam grew quickly, and Ponzi pocketed nearly $20 million before he skipped the country and left investors to realize their losses.

Ponzi's scam is extremely helpful in understanding fraud. Certainly, the scheme involved deception. It also involved greed - greed by the perpetrator - and this is important, even greed by the investors, who wanted higher-than-sensible returns. Finally, Ponzi's scheme involved the element of confidence. If he had not paid the original $300 "returns," investors wouldn't have invested additional money. By paying early "returns," Ponzi gained investors' confidence and convinced them that he had a legitimate business. In fact, confidence is the single most critical element for a fraud to be successful. (The word "con," which means to deceive, comes from "confidence.") It is difficult to con anyone out of anything unless the deceived has confidence in the deceiver. One cannot be conned unless one trusts the person trying to deceive him. Similarly, employers cannot con employees if they do not have their employees' trust and confidence. And, without investor confidence, fraudulent companies cannot con unsuspecting investors.

4. Types of Fraud

The most common way to classify fraud is to divide frauds into those committed against an organization and those committed on behalf of an organization.

In occupational fraud – fraud committed against an organization –the victim of the fraud is the employee's organization. The Association of Certified Fraud Examiners defines this type of fraud as, "The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets. Occupational fraud results from the misconduct of employees, managers, or executives. Occupational fraud can be anything from lunch break abuses to high-tech schemes. The Report of the Nation in Occupation Fraud and Abuse by the Association of Certified Fraud Examiners states that, "The key to occupational fraud is that the activity (1) is clandestine, (2) violates the employee's fiduciary duties to the organization, (3) is committed for the purpose of direct or indirect financial benefit to the employee, and (4) costs the employing organization assets, revenues, or reserves."

Frauds can be divided into the following six types:

- Employee embezzlement.
- Management fraud.
- Investment scams.
- Vendor fraud.
- Customer fraud.
- Miscellaneous fraud.

Detail explanations are in Table 1.

Table 1 : TYPES OF FRAUD

Type of Fraud	Victim	Perpetrator	Explanation
• Employee embezzlement or occupational fraud	Employers	Employees	Employees directly or indirectly steal from their employers.
• Management Fraud	Stockholders, lenders, and others who rely on financial Information	Top management	Top management provides misrepresentation, usually on financial statements.
• Investment scams	Investors	Individuals	Individuals trick investors into putting money into fraudulent investments.
• Vendor fraud	Organizations that buy goods or services	Organizations or individuals that sell goods or services	Organizations overcharge for goods or services or non-shipment of goods, even though payment is made.
• Customer fraud	Organizations that sell goods or services	Customers	Customers deceive sellers into giving customers something they should not have or charging them less than they should.

5. Who commits fraud?

Past research has shown that anyone can commit fraud. Fraud perpetrators usually cannot be distinguished from other people by demographic or psychological characteristics. Most fraud perpetrators have profiles that look like those of other honest people.

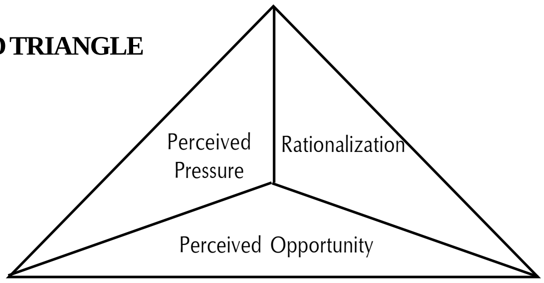
5.1 Profiles of Fraud Perpetrators

It is important to understand the characteristics of fraud perpetrators because they appear to be much like people who have traits that organizations look for in hiring employees, seeking out customers and clients, and selecting vendors. This knowledge helps us to understand two things: (1) most employees, customers, vendors and business associates and partners fit the profile of fraud perpetrators and are probably capable of committing fraud and (2) it is impossible to predict in advance which employees, vendors, clients, and customers will become dishonest. In fact, when fraud does occur, the most common reaction by those around the fraud is denial. Victims can't believe that individuals who look and behave much like them and who are usually well-trusted can behave dishonestly.

6. Why people commit Fraud ?

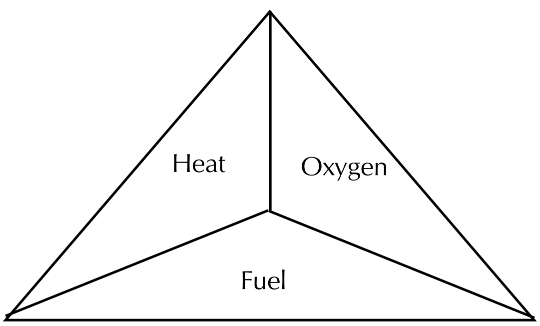
Although there are thousands of ways to perpetrate fraud, there are three key elements common to all of them (1) a perceived pressure, (2) a perceived opportunity, and (3) some way to rationalize the fraud as acceptable. These three elements make up what we call the fraud triangle. (Figure 1)

Figure 1 : THE FRAUD TRIANGLE



Fraud resembles fire in many ways. For fire to occur, three elements are necessary (1) oxygen, (2) fuel, and (3) heat. These three elements make up the "fire triangle," as shown in Figure (2) When all three elements come together, there is fire.

Figure 2 : THE FIRE TRIANGLE



Firefighters know that fire can be extinguished by eliminating any one of the three elements. Oxygen is often eliminated by smothering, by using chemicals, or by causing explosions, as is the case in oil well fires. Heat is most commonly eliminated by pouring water on fire. Fuel is removed by building fire lines or fire breaks or by shutting off the source of the fuel.

As with the elements in the fire triangle, the three elements in the fraud triangle are also interactive. With fire, the more flammable the fuel, the less oxygen and heat it takes to ignite. Similarly, the purer the oxygen, the less flammable the fuel it needs to ignite. With fraud, the greater the perceived opportunity or the more intense the pressure the less rationalization it takes to motivate someone to commit fraud. Likewise the more dishonest a perpetrator, the less opportunity and/or pressure it takes to motivate fraud.

People who try to prevent fraud usually work on only one of the three elements of the fraud triangle – opportunity. Because fraud-fighters generally believe that opportunities can be eliminated by having good internal controls, they focus all or most of their preventive efforts on implementing controls and ensuring adherence to them. Rarely do they focus on the pressures motivating fraud or on the rationalizations of perpetrators.

It is worthwhile to examine the elements in the Fraud Triangle in more detail.

6.1 Perceived Pressure

Most experts on fraud believe these pressures can be divided into four types (1) financial pressures, (2) vices, (3) work-related pressures, and (4) other pressures.

- **Financial Pressures**

  - Greed
  - Living beyond one's means
  - High bills or personal debt
  - Poor credit
  - Personal financial losses
  - Unexpected financial needs

- **Vice**

Closely related to financial pressures are "vices" – addictions such as gambling, drugs, and alcohol – and expensive extramarital relationships. As an example of how these vices motivate a person to commit fraud, one should listen to an individual's confession of how gambling led to his dishonest acts.

- **Work-Related Pressures**

Whereas financial pressures and vices motivate most frauds, some people commit fraud to Figure 1 : THE FRAUD TRIANGLEget even with their employer. Factors such as not enough recognition for job performance, dissatisfaction with the job, fear of losing one's job, being overlooked for promotion, and feeling underpaid motivate many frauds.

- **Other Pressures**

Once in a while, fraud is motivated by other pressures, such as a spouse who insists on an improved lifestyle or a desire to beat the system.

6.2 Perceived Opportunity

A perceived opportunity to commit fraud, to conceal it, or to avoid being punished is the second element in the fraud triangle.

At least six major factors increase opportunities for individuals to commit fraud in organizations. The following list is not exhaustive, but it does show the weaknesses of the system that create opportunity.

- Lack of or circumvention of controls that prevent and/or detect fraudulent behaviour.
- Inability to judge quality of performance.
- Failure to discipline fraud perpetrators.
- Lack of access to information.
- Ignorance, apathy, and incapacity.
- Lack of an audit trail.

6.3 Rationalization

Nearly every fraud involves rationalization. Most perpetrators are first-time offenders who may not have committed other crimes. Rationalizing helps them hide from the dishonesty of their acts. Here are some common rationalizations used by fraudsters:

- The organization owes it to me.
- I am only borrowing the money – I will pay it back.
- Nobody will get hurt.
- I deserve more.
- It's for a good purpose.

- We'll fix the books as soon as we get over this financial difficulty.
- Something has to be sacrificed – my integrity or my reputation.(If I don't embezzle to cover my inability to pay, people will know I can't meet my obligations and that will be embarrassing because I'm a professional.)

7. Fraud Symptoms

- ***Accounting anomalies.***
  Because accounting records are often manipulated to conceal fraud, anomalies and problems with accounting documents – either electronic or paper journals, ledgers, or financial statements are sources in identifying symptoms of fraud.

- ***Internal control weaknesses.***
  One of the main purposes of internal control procedures is to safeguard assets. When controls are absent or weak (or overridden), they facilitate fraud.

- ***Analytical anomalies.***
  These are relationships, records, or actions that are too unusual or unrealistic to be believed. They include transactions or events that happen at odd times or places, activities that are performed by, or involve people who would not normally participate in them, as well as peculiar procedures and policies. Other anomalies that should be scrutinized carefully include amounts that are too large or too small, that occur too often or too rarely, or that result in excesses or shortages.

- ***Lifestyle symptoms.***
  Once perpetrators meet the financial needs that motivated them to commit fraud, they usually continue to steal and then use the money to enhance their lifestyles. They may buy expensive cars or other personal items, take extravagant trips, remodel their homes or purchase more expensive ones, or buy expensive jewellery or clothes.

- ***Unusual behaviours.***
  When people commit crimes (especially first-time offenders, as many perpetrators are), they are engulfed by feelings of fear and guilt. These emotions express themselves in unusual behaviour. There is not one particular behaviour that often signals fraud; rather, it is a pattern of changes in behaviour. People who are accommodating, become intimidating and belligerent; people who are belligerent become easy to work with, and so forth.

- ***Tips and complaints.***
  People who are in the best position to detect fraud are usually those closest to the perpetrator – family members, friends, co-workers, managers, and others, not the audi-

tors or fraud examiners. These individuals often provide tips or complaints that suggest that fraud is being committed. Although such complaints and tips are often legitimate, they can be motivated by a desire to get even, by frustration or personal vendettas, or by numerous other reasons.

8. Fraud Risk Assessments

Traditional risk assessments link risks to the organization's key objectives. Therefore, fraud can be overlooked during this type of review if it is not considered a core company objective.

Fraud risk assessments also examine existing controls, but focus specifically on control measures aimed at preventing or detecting fraud. The assessments investigate whether or not controls can be circumvented and consider the susceptibility of controls to man agement override.

Most importantly, fraud risk assessments concentrate on fraud schemes and scenarios. Assessments aim to identify activity that can: a) significantly impact the organization's reputation, (b) expose the company to criminal or civil liability, or (c) result in a financial loss. Assessment teams must be able to identify all the potential schemes and scenarios impacting the industries and geographic markets in which the organization conducts business.

8.1 Fraud Risk Assessment Process

Fraud Risk Assessment Process can be enumerated as below and this process can be followed not only by Auditors but a team of management including business and other key process owners with the sponsorship and approval for Risk assessment process by the Board of Directors.

- ***Organize the assessment***
  Fraud risk assessment process can be organized with the sponsorship from the top management.

- ***Determine areas to assess***
  To be effective, fraud risk assessments must be conducted at companywide, business unit, and significant account levels.

- ***Identify potential schemes and scenarios***
  Organizations can be defrauded, or commit fraud, in myriad ways. Identifying the organi zation' s universe of potential fraud risks, therefore, represents a critica stage of fraud risk assessment.

- ***Assess likelihood of Fraud***
  Fraud risk assessments, like traditional risk assessments, consider the likelihood that a particular fraud will occur. Risk likelihood levels are defined as:

  - Remote
  - More than remote or reasonably possible
  - Probable

- ***Assess significance of Risk***
  After determining the likelihood of possible frauds, auditors should assess the significance of fraud risks with a more than remote likelihood of occurring. In this context, use the following criteria:

  - Inconsequential
  - More than inconsequential
  - Material

- ***Link Antifraud Controls***
  Once fraud risks have been assessed, identify the control activities for fraud risks that are both more than remotely likely to occur and more than inconsequential in amount.

8.2 Analysing Fraud Risks

Fraud risk is one component of operational risk. Operational risk focuses on the risks associated with errors or events in transaction processing or other business operations. A fraud risk review considers whether these errors or events could be the result of a deliberate act designed to benefit the perpetrator. As a result, fraud risk reviews should be detailed exercises conducted by teams combining in-depth knowledge of the business and market with detailed knowledge and experience of fraud.

Risks such as those of false accounting or the theft of cash or assets need to be considered for each part of the company's business. Frequently, businesses focus on a limited number of risks, most commonly on third-party thefts. To avoid this, the risks should be classified by reference to the possible type of offence and the potential perpetrator(s). The following matrix developed by Ernst and Young ('the Ernst and Young model') can be used.

Department/ Collusion area	Details of risk area	Management	Employees	Third parties
False accounting				
Theft				

8.3 Fraud Risk Mitigation

A Company's system of internal control has, as its principal aim, the management of risks that are significant to the fulfillment of its business objectives with a view to safeguarding the company's assets and enhancing over time the value of the shareholders' interest.

Having an effective control structure is probably the single most important step organizations can take to prevent and detect employee fraud or mitigation of fraud risk. There are three components in a company's control structure (1) the control environment, (2) the accounting system, and (3) control procedures or activities.

Detailed explanations are in table 2, below

Table 2 : INTERNAL CONTROL STRUCTURE

Control Environment	Accounting System	Control Activities or Procedures
- Management philosophy and operating style, modeling - Effective hiring procedures - Clear organizational structure and communication - Effective internal audit risk management	- Valid transactions - Properly authorized - Completeness - Proper classification - Proper timing - Proper valuation - Correct summarization	- Segregation of duties - Proper procedures for authorization - Adequate documents and records - Physical control over assets and records - Independent checks on performance

8.4 Responsibility for Fraud Risk Management

The primary responsibility for the prevention and detection of fraud and error rests with both the management of an entity and those charged with the governance of that entity.

It is the responsibility of the management of an entity to establish and maintain policies and procedures to assist in achieving the objective of ensuring, as far as possible, the orderly and efficient conduct of the entity's business. This responsibility includes implementing and ensuring the continuity of operation of accounting and internal control systems which are designed to prevent and detect fraud and error. Such systems reduce but do not eliminate the risk of misstatements, whether caused by fraud or error.

It is the responsibility of those charged with governance of an entity to ensure through oversight of management, the integrity of an entity's accounting and financial reporting systems and that appropriate systems of control are in place, in particular, systems for monitoring risk, financial control and compliance with the law.

9. Frauds in Banks

More familiar frauds in banking sector are indicated with some of the measures that a bank could adopt to mitigate risk of such frauds.

9.1 Credit Frauds

Cash advances, against pledged goods, as security, are a fertile field for frauds.

Employees/officers of organizations perpetrate credit frauds in connivance with prospective borrowers or on their own or due to other pressures. The evaluation of credit worthiness of customer is carried out manipulating the factual position to approve larger facilities. Common contributors to credit frauds are inadequate/or lack of security to cover risk and lack of proper credit documentation. As a result the recovery of the dues from the borrowers becomes difficult/impossible.

9.1.1 Credit Fraud Risk Mitigation

Risk mitigatory measures mainly include:

- Training and developing staff in credit.
- Enhancing Internal Controls
- Encouraging independent review of credit operations, and
- Designing exceptional reports to identify the deficiencies/fraudulent activities
- Physical verification of securities and periodic inspection
- Examination of audited financial statements.

9.2 Cheque Frauds

Cheque frauds include frauds relating to customers' cheque's, banker's cheques (drafts) or traveller's cheques. They are the most critical frauds both loss-wise and volume-wise.

- Counterfeit bank drafts, traveller's cheques and other cheques
- Forging signatures alteration of cheques information.
- Impersonation.
- Opening fictitious accounts for the purpose of using this as a vehicle for committing fraud.

Some banks open accounts without adherence to the basic requirements. Such as Know Your Customer Concept (KYC) requirements. Some banks had even guaranteed the fate of proceeds of fraudulent cheques to be collected.

9.2.1 Cheque Fraud Risk Mitigation

- Strengthening the KYC policies/standards
- Obtaining Identity Cards and two Utility Bills.
- Obtaining an independent confirmation of the address from the referees or via sending a registered welcome letter.
- Standardizing the format and procedures to be followed by all Banks in opening of accounts.
- Balance confirmation on periodic basis.

9.3 Frauds in Deposit Accounts (Dormant/In-operative/Closed Accounts)

These accounts are highly vulnerable for frauds. Signature information leakage is a major contributor to fraudulent withdrawals. This can be done with the connivance of the internal staff or the carelessness of the customer.

9.3.1 Deposit Accounts Risk Mitigation

- Signature cards should be well protected against improper use.
- Secure custody of cheque book, Pass books and other documents.
- Increasing internal controls with regard to payment/release of funds.
- Systematic control for dormant inoperative accounts.
- Independent checks/Surprise checks and Balance Confirmations

9.4 Insider frauds (Banker's Bunks)

A dishonest banker can play havoc with the bank's money. The bank has, therefore, to guard itself and its customers against the dishonest employee.

- Manipulation of cash by those handling cash.
- Misappropriation of customers deposit accounts.
- Misappropriation of money, mail and telegraphic instruments/transfers.

With mail interception with inside or outside assistance and thereafter issue of instructions to the bank to execute fraudulent transactions or by stealing payment instrument is a common fraud.

This interception can take place from the point of issue of the letter/cheque by the customer up to the bank which receives letter/cheque where the account is maintained. More frauds connected to NRFC accounts are committed by this modus operandi.

9.4.1 Insider Fraud Risk Mitigation

- Verifying the authenticity of the limits/making inquiries from the customer where suspi cions are aroused.
- Designing exception reports.
- Granting limits to each segment of operations.
- Independent checks/surprise checks
- Protecting customer sensitive information such as signatures i.e. limiting access.

9.5 Frauds due to Outsourcing

Outsourcing has three main risks (1) Legal Risk .2) Security Risk. 3) Dependence/Exit Barrier risk. Hence more care is required to protect unauthorized access to signatures of accounts on sensitive documents etc. by outside personnel.

9.5.1 Outsourcing Fraud Risk Mitigation

- Formal Contract
- Proper Data Security
- High level monitoring
- Performance measures

9.6 Frauds connected to ATMs

There is a high tendency to obtain customer-sensitive information using high tech devices in ATMM to perpetrate fraud.

9.6.1 ATM Fraud Risk Mitigation

- CCTV cameras at ATM locations in order to monitor the utilization.
- Paper Journal Recording.
- Physical Security Measures.

9.7 Credit Card Frauds

Frauds by individuals include unauthorized use of lost or stolen cards, counterfeit cards, skimming, fraudulent credit card application and frauds via Internet. Frauds by merchants include generating false sales claims and accepting transactions knowingly by unauthorised persons.

9.7.1 Credit Card Fraud Risk Mitigation.

- Customer awareness.
- Stringent control measures for enrolment of customers/merchants.

9.8 Issuance of Fraudulent Bank Guarantees/Letters issued to Embasies Conforming Customer Balances

The nature of these instruments is such that the bank will not realize the fraud till a claim is maid or confirmation sought.

9.8.1 Bank Guarantee/ Balance Confirmation Fraud Risk Mitigation

- Customer awareness.
- Use of security documents.

10. Preventative Measures

Apart from the specific mitigatory measures there is a need to implement a proper risk Management Programme which covers the following :

10.1 Developing an Anti-Fraud Culture

Attitudes within an organization often lay the foundation for a high-or low-risk environment. Where minor unethical practices may be overlooked (e.g. petty theft, expenses frauds), larger frauds committed by higher levels of management may also be treated in a similar lenient fashion. In this environment there may be a risk of total collapse of the organization either through a single catastrophic fraud or, through the combined weight of many smaller frauds. Therefore in banks the attention towards frauds need not leave room for leniency.

Emphasizing the importance of building up of a culture to pick up early warning signals on arising risk in all areas by the Banks is of paramount importance. A Fraud Risk Policy approved by the Board of Directors is essential.

10.2 Risk Awareness

Almost every time a major fraud occurs, many people who were unwittingly close to it are shocked that they were unaware of what was happening. Therefore, it is important to raise awareness through formal education and training programmes as part of the overall risk management strategy. Particular attention should be paid to those managers and staff operating in high-risk areas, such as cash and account operation, and to those with a role in the prevention and detection of fraud, for example audit, human resources and staff with investigation responsibility.

10.3 Whistle Blowing

The importance of a whistle blowing system by internal staff of banks to combat fraudulent activities needs no emphasis. It is essential that a framework be designed to accommodate such a situation and to protect the source of information.

10.4 Common Mitigatory Measures

- Deposits of staff to be reviewed/monitored by a senior officer.
- Assets of staff to be regularly reviewed with declarations made by the staff members.
- Sudden changes of life styles of employees too to be observed and identified.
- Sending staff on at least 7 day continuous leave is essential, especially for Managers / Heads of Units and posting independent persons to perform their functions.
- There should be releasing arrangements for senior officers in Head office, Treasury, Trade Finance when on leave.
- Rotation of staff within departments/sections/branches on a regular basis.

11. Conclusion

Fraud is common not only to banks but to many organizations and even to society in general. What needs to be understood is why people commit frauds and to minimize the oppportunities for committing fraud specially by following up on fraud symptoms. As banks are dealing with depositors' cash, fraud risk management is a high priority in the Agenda of the Management of banks.

References :

1) Institute of Internal Auditors, USA – Journals and - website www.theiia.org.
2) Association of Certified Fraud Examiners, USA website - www.acfe.org.
3) American Institute of Certified Public Accountants, USA-website- www.aicpa.org
4) Information Systems Audit and Control Association, USA-website www.isaca.org

BLANK