

# Fraud in business: an expensive hobby

*Fraud is a deliberate misrepresentation of evidence which causes another person or organisation to suffer damages, usually monetary losses. There are at least as many types of fraud as there are types of people who commit it. Fraud costs the economy an enormous amount. Fraud happens when somebody uses deception to obtain goods, services or money.*

Fraud is one of businesses biggest plagues that can unknowingly cripple the organisation if not detected and eradicated. The dictionary meaning of fraud is a criminal deception, dishonest trick, impostor, disappointing person, etc.

Fraud is a deliberate misrepresentation of evidence which causes another person or organisation to suffer damages, usually monetary losses. There are at least as many types of fraud as there are types of people who commit it. Fraud costs the economy an enormous amount. Fraud happens when somebody uses deception to obtain goods, services or money.

The following are some of the examples of fraud:

- misappropriation of funds,
- theft of cheques,
- overriding decline decisions so as to open accounts for family and friends,
- inflating expense claims,
- pretending relatives have died to take bereavement leave,
- forging signatures,
- removing money from customer accounts,
- falsifying documents,
- selling company assets at below their true value in return for payment,
- deliberately steering supplier contracts to relatives,
- bribery,
- computer fraud,
- white collar fraud.

## Characteristics of fraud

Unlike crimes that can be detectable by physical evidence, employee fraud may be difficult to detect because often only symptoms of such crimes are readily apparent and the symptoms may or may not signal actual fraud. Employee fraud is a crime that is almost never observed directly.

When someone is murdered, there is little question that a crime has occurred because of the presence of clear physical evidence. The corpse can be touched, seen

and even smelled; the specific unnatural cause of death can be identified by the medical examiner.

When a bank is robbed, there is first-hand evidence from eye witnesses, both customers and employees. Frequently, there is a videotape recording of the entire episode that can be replayed for any doubters.

But when an employee commits a fraudulent act against his or her employer, there generally is no direct evidence that a crime has been committed; there are only symptoms, 'red flags' or indicators of fraud.

Motive and opportunity are essential components for fraud to occur. Most people who commit fraud are under financial pressure. Sometimes, these pressures are real; other times, they are excuses for greed.

Once perpetrators of fraud meet their immediate financial needs, they usually continue to steal and use the embezzled funds to enhance their lifestyles. Often, they buy an expensive car or other extravagant toys, take extravagant trips, remodel their existing homes or purchase more expensive ones, buy expensive jewellery or clothes or just start spending more on standard living expenses.

For fraud to be sustained, the guilty employee typically must also rationalise the behaviour. Weak internal controls and/or collusion with colleagues or outside third parties usually create opportunities. The focus of an organisation's fraud and integrity risk management programme should commence by defining the various opportunities that exist in conducting fraud.

Rationalisation is the process by which the person committing a fraud legitimises his or her crime to them self. This often includes a feeling of entitlement and a belief that 'the company can afford it.'

Auditors cannot easily detect fraud when the actual theft takes place because fraudulent activities most likely will not happen while they are present. Certainly,

during the one or two weeks each year auditors spend time conducting their audits, then theft and fraud usually stops. It is difficult for auditors to detect, for example, that an employee who used to drive a used, inexpensive car now comes to work in a brand new expensive model or that an employee suddenly expresses changes in behaviour.

Auditors do have a chance to find fraud if their audit samples include altered documents, miscounts or other anomalies. However, co-workers, friends and managers are in a better position than auditors to detect fraud at any time.

Unfortunately, these individuals who are most likely to detect the symptoms of employee fraud have not been trained to recognise these symptoms. Many fraudulent acts, in fact, are detected as the result of a tip or complaint made by an employee, friend, manager or customer.

The rate of employee theft is increasing in every segment of the industry and businesses are losing millions of Rands as a result. The detection of fraud by employees requires that managers, auditors and co-workers recognise the symptoms that suggest a crime may have been committed.

They must remember that the symptoms of fraud are neither predictive nor absolute. For example, only one symptom may be present in a particular case of fraud; in another case, numerous symptoms may be present even though fraud is not occurring. A full investigation of all symptoms nevertheless is necessary to determine whether or not an employee is engaging in fraudulent activities.

## Fraud warning signs

The following behaviour changes of staff are some of the typical warning signs that may require some careful investigation:

- staff under stress without a high workload – marked personality changes,
- always working late,

- reluctance to take leave,
- unexplained wealth or living beyond apparent means,
- sudden change of lifestyle,
- customer complaints of missing statements, unrecognised transactions,
- new staff resigning quickly,
- cosy relationships with suppliers, contractors or customers,
- suppliers or contractors who insist on dealing with just one individual,
- rising costs of business with no explanation,
- key employees having too much control or authority without audit checks,
- employees with external business interests,
- Employees getting into debt,
- certain employees who are always disgruntled,
- employees who have drug habits,
- an employee who refuses promotion,
- an employee who chooses a hidden work environment,
- an employee who takes frequent smoke breaks or trips to the toilet.

## Impact of fraud

### *Financial loss*

Financial fraud is defined as a deliberate act or failure to act that is contrary to law, rule or policy with the intent to obtain unauthorised financial benefit from the organisation for oneself, one's family or one's business associates.

Financial fraud includes, but is not limited to, misappropriation of an organisation's funds or property, authorising or receiving compensation or reimbursement for goods not received or services not performed or hours not worked or unauthorised alteration of financial records.

These losses will impact directly on the company's bottomline. Some international studies have shown that losses due to fraud can equate to an average of 20% to 40% of annual profits.

### *Reputational damage*

There is always media interest in fraud and this can be damaging to organisations that depend on a high level of confidence from their customers.

### *Internal damage*

Incidents of fraud will have a substantial internal impact on business. There will be added costs of investigation and disciplining, and replacement costs if there are dismissals. Cases of fraud can lead to a negative impact of morale and trust between co-workers which will disrupt the normal routine of doing work.

Speculation, misinformation, rumours and gossip can also create a culture of mistrust and suspicion. Team spirit and morale can be harmed if employees are shocked and unsettled when one or more



*Roy Ramphal is President of SAATCA – the South African Association of Quality Auditors – and the South African Society for Quality and he lectures at the University of Johannesburg.*

of their members are dismissed, arrested or prosecuted.

## Combating fraud

It is very difficult to predict that fraud will be totally eliminated, but rather to have an awareness of detecting them and implementing preventative measures. Some of these measures include:

### *Code of ethics*

Every organisation should have a code of ethics which must be well communicated and entrenched. It is considered good practice to introduce an induction programme for all new employees educating them on what the company policies are and where they can be located within the company, usually on a display board in an open area.

### *Staffing changes*

Rotate employees who are in positions dealing with major customers and suppliers. This will minimise the formation of cosy relationships. This could apply to buyers, creditor clerks, salesmen and debtors staff.

Change service contractors who are in positions that require a high level of trust. For example some organisations change

their security service providers on an annual basis.

### *Monitoring of staff turnover*

Staff turnover revolves around resignations or terminations? The effective measurement of staff turnover could be used as an indicator to ask further questions. When the questions have been answered some fraudulent activities might be found to be the root cause as employees resign before they are caught or drawn into a syndicate involved in fraud.

### *Recruitment screening*

A company can immediately reduce its fraud risk if it can effectively screen its new candidate employees and not hire them if it is found that they have been involved with unethical practices. Most companies should insist on the provision of supporting documents and verify them before confirming the appointment of the candidate.

This should apply to all candidates irrespective of position and status and to all types of employment (casual, temporary and permanent employment). In addition, the interview should be in terms of a panel interview or the candidate be interviewed by at least twice with different interviewers.

### *Compensation level*

If employees are compensated less than a fair industry benchmark, they might be forced to make up the difference through unethical practices. It is therefore required that periodical benchmarks are made regarding compensation levels to ensure a highly motivated ethical staff.

### *Avoid crisis management*

In most cases normal procedures are overlooked when engaged in crisis management. The crisis mode can be an ideal breeding place for fraud. Usually if the unethical incident is not covered up and the individual is caught, he or she might just plead ignorance due to the current environment and undue pressures of getting the work done.

### *Appropriate disciplinary action*

The organisation needs to demonstrate its commitment to ethical behaviour by ensuring there is a fair disciplinary code with appropriate sanctions against those who are found to be transgressing the code of conduct.

The various managers must be 'strong' and committed to investigate or support any external investigation of suspicions of fraud. Managers who shy away from this process must be seen to promote a culture of fraudulent activities.

### *Internal controls*

The organisation should have all their processes analysed for risk and implement appropriate controls to minimise them.

### *Review of audit results*

Management should critically analyse auditor reports or conduct further investigations into the items reported to ensure that the respective processes are 'fraud free.' Some examples of auditor items that might indicate fraud are:

- Discrepancies in accounting records, i.e., account balances that are significantly over- or understated, transactions not recorded in the proper manner and last minute account adjustments.
- Poor audit trail, missing documents, unexplained reconciliations, inconsistent or vague responses to queries, missing inventory or physical assets, inexplicable changes to documents specifically hand written and duplication of payments.
- Unusual client relationship when auditors are denied access to records, facilities, certain employees, customers and suppliers.

### *Policy on gifts and gratuities*

There should be clear guidelines on the receiving of gifts and gratuities from suppliers and customers. An example would

be that when a gift is received from a supplier that the buyer involved must document it in a register and have it approved by his manager. This ensures that everything is transparent.

### *Regular stock takes*

Inventory is the heart of many organisations; hence it should be subjected to frequent stocktakes conducted by internal and external staff. Inventory can be subdivided into different sections based on product type, location, value, etc.

Stocktake activities can be done weekly, rotating the different sections each time. All stock write offs should be done with adequate investigation.

### *Fraud reporting structure*

The organisation should create appropriate structures for the reporting of any fraudulent activities. One such structure is whistle blowing. The company must communicate this structure publicly so that their structures are not just available for internal employees, but also open to external parties.

However, the communication and structures must ensure that they protect and support those that expose fraud, corruption, dishonesty and any unethical behaviour of its employees.

### *Unpredictable audits*

Sometimes when auditors are predictable, fraudsters actually prepare themselves. Some reported examples include:

- If the fraudster knows that the auditor will be looking at a certain site, he will transfer 'hot goods' to another site.
- The fraudster fills water into containers indicating that it is full with product to compensate for containers of product that are missing.

Hence, unpredictable audits are those where the fraudsters cannot predict the areas or processes the auditor will choose for the audit. This will increase the chances of the auditor detecting fraud if it exists. This action will also reduce the opportunities for fraud because there will be a higher likelihood of detection.

Some of the methods to institute unpredictable audits include random sampling, unannounced site visits, changing the dates of audits, changing audit techniques year to year, include low risk areas and processes, observe discreetly, sample whistleblower complaints, include customer/supplier correspondence and include interviews with employees who have left the organisation.

### *Multidiscipline audits*

The organisation should not only be subjected to just financial audits. Other audits, for example, include quality, environment, health and safety, security and IT. Fraud can also be identified with these

types of audits.

### *Processes and procedures*

The organisation should have well documented processes and procedures and ensure that there are well trained on them.

### *Healthy environment*

I refer to a 'healthy' environment as one where the work place is well lit up, adequate ventilation, work well organised, clean and with a strong culture of tidiness. Fraudsters take advantage of work areas where information and products can be hidden and where is a lot of sloppiness in getting work done.

An interesting model that can be used to promote a 'healthy' work environment is the '5s' model which has the following steps:

- *Sort*: remove all items that are no longer required in the work place. Examples of such items includes redundant materials in the warehouse, customer rejections, redundant processes, redundant documents, redundant computer files, etc.
- *Set*: arrange items so that they are easy to retrieve and store after use.
- *Shine*: ensure that the work area is wiped, shined and looking clean. This might include the racking in the stores, windows, various floors and various tools and equipment.
- *Standardise*: this way of housekeeping must become a culture and must be integrated into the processes and procedures of the organisation.
- *Sustain*: management must provide the motivation and reinforcement of such behaviour by providing housekeeping awards, special bonuses.

### *Good waste removal services*

The organisation needs to have an adequate wastage removal system with credible removal partners to ensure that the wastage does not unknowingly end up with wrong parties.

A company was found to be defrauded after relevant financial information was thrown unheeded into a rubbish bin and transported out of the factory. One of the employees of the wastage company passed the information to some fraudsters.

Another company lost expensive raw materials which was found to be transported out of the warehouse with the daily rubbish collected.

## **Conclusion**

Fraud is not an easy area to detect hence management needs to adopt a 'prevention' approach rather than a 'cure' approach. This article gives some insight into the definition, the characteristics, the impact and some recommendation on combating it. ■