The Forensic Accountant

The Forensic Accountant Handbook is compiled by CDIMS for Seminar on Forensic Audit, Mumbai. The participants will find this handbook useful as it contains discussion on various types of frauds and method/ techniques to detect them.

The Forensic Accountant's Hand Book

Compiled by Chetan Dalal, Mahesh Bhatki,
Jatin Jhaveri, Rajan Gupte and Govindsingh Purohit

Contents

Notice and Disclaimer

Without the prior consent of the author, no part of this compilation may be copied, reproduced, stored or transmitted in any form or by any means including without limitation by means of electronic, mechanical, photocopying, recording or otherwise. The opinions and views expressed in this compilation are without prejudice and are based on experience of the authors, research or based on empirical studies. The material is purely for academic educational purposes and should not be construed as professional advice. The author does not warrant that the views stated shall be effective in each and every case or may give predictable consequences. The author shall not be responsible for the result of any action taken on the basis of this work whether directly or indirectly and for any errors or omissions in the work. The authors expressly disclaim all and any liability and responsibility to any reader of whatsoever in nature. References to names in this handbook are merely fictional / imaginary and their resemblance to any living or non-living things, people or organizations are purely coincidental.

Chapter 1. **Early Warning Bells, red flags and common fraud scenarios**

In modern times fraud is not only rampant but also exponentially large in magnitude. This is because perpetrators of fraud are an intellectual lot and have the ability to camouflage their wrongdoings. Consequently, whenever any important decision is to be taken, be it budgeting, financial cash flows or even high-level corporate decisions such as takeover or mergers, project appraisals or any financial major commitment, the specter of fraud, deception and overall risk looms high. The key issue is therefore to have some system of discerning early warning bells or to apply methods to spot red flags of potential risk, before taking any major step forward. No doubt, lot of effort in due diligence exercises is being put in, but more often than not, there are glaring omissions which are very clear only when disaster eventually strikes and it is too late. Is there a way to minimize such risk and to enhance the probability of nipping fraud in its initial stages?

Funnily enough there is no great rocket technology involved. Generally speaking, it is more or common sense, logic and a whole lot of patience in absorbing and digesting information available. The central thrust is to detect anomalies and inconsistencies. However, to be a little more specific, there are some simple commonplace red flags which most fraud investigators look for in scenarios of financial evaluations and some of them are explained below. If these red flags are hunted or searched for in financial reviews, even in audits, the probability of fraud being detected in early stages would be significantly greater.

1. ***Hunting for secret reserves***. There could be situations where funds are masked or hidden. This could be done for any reason such as concealing the correct fund position, or for keeping funds aside for future misuse or embezzlement. Such practices can also be applied to give an incorrect position during takeovers, mergers or other instances of recovery of defaulting borrowers. Perpetrators of fraud use infinite number of ways to hide such funds. The most common way is to make illusionary payments or payments to fictitious parties. The effect of such payments is to reduce the bank balance in the financial accounts, but in reality, since there is no payee there is no one to present the cheques. Consequently, the funds are very much there, which can be embezzled at a later date when the opportunity arises. What are the red flags which can be hunted for to reveal secret reserves? There are several. The first and the most revealing method is to determine whether there are stale cheques in the system. Stale cheques are cheques issued to payees who have not

presented the cheques for payment for over six months. As we all know a cheque become invalid six months after the date of its issue. Such stale cheques are secret reserves if they appear in the bank reconciliation statement (BRS). BRS is a simple comparison and reconciliation statement between the balance as shown in the bank statement (bank passbook) and the cash book maintained by the entity. All cheques issued by the entity *but not presented by the payees* will appear as unreconciled entries in the bank reconciliation statement. Stale cheques remain unquestionably secret reserves as long as they appear in the bank reconciliation statement. They cease to be secret reserves only after they are removed from the BRS by an appropriate accounting done in the books of account, which is seldom done. This secret reserve concept can be further extended even to such unpresented cheques more than one month old, because there is a 90 % chance that these payees are non-existent or that they have not been handed over these cheques for ulterior motives. Therefore every due diligence exercise would do well to ask for a complete list of bank accounts in use and bank statements for each of these must be examined along with the BRS for secret reserves as explained above. Another method of hunting for secret reserves is a study of the liabilities to third parties. Very often perpetrators create liabilities in books without any sound basis. The intention could be to show a lesser profit, or to create an incorrect liability for future encashment through accomplices at an opportune time. Red flags can be spotted by studying accounting behavior of creditors and third parties. Imagine if vendors, suppliers or creditors do not ask for payment of large amounts due to them as per the books of account, for months together- is this possible in recessionary conditions? Unlikely. Such dormant or well behaved creditors are illusionary. A simple scrutiny of third party payables will clearly show those who are reluctant to ask for payments. More often than not these are not really payable.

2. ***Distinguishing exaggerated expenses or business losses from underlying techniques of siphoning out of funds***

   There are also ways and means adopted by perpetrators of fraud for duping investors and equity partners or potential acquirers of business. Exaggerated incomes, sales, receipts and/or deflated expenses are very possible. This is done with a view to improve the share prices at the time of the takeover. There are ingenious ways of doing this. In one unique case, where the takeover of a business was to be spread over three years, the previous management was told that company taking over had a norm of permitting a maximum of 3 % loss on account of rejections or wastage. However little did that company realize that it gave away an important piece of information- that it tolerated 3 % rejection *which was much higher* than that of the previous management whose company was being acquired was much lower at about 0.25% because of a slightly better kind of machine. Needless to state the previous management exploited the situation fully and during the phase wise takeover period in 3 years during which they had the operating authority, they smoothly and covertly creamed off the difference of 2.75 % rejection which in absolute terms ran in to several crores of rupees. Such malpractices can happen in myriad number of ways. How can one really spot these manipulations? Admittedly it is very difficult. However, these need lucid thinking and a multi-pronged approach. Apart from financial and legal due diligence, there need to be certain important key factors to be probed into for each industry- gross margin, wastage, yield and inventory ratios etc. More importantly the due diligence must continue even during the takeover process (using intelligence agencies), and for some time after the takeover till such time that the new management completely takes over. This is to protect and inform the new management of business diversion, opportunities lost or transferred to other entities, and other abuses which take place in a big way even through old loyal employees. Use of 'moles' as employees, suppliers or third parties can also be useful .

3. **Spotting illusionary revenues and profits.**

This is perhaps the most difficult. This can be done in two broad ways: inflation of income or deflation of expense. In many cases the expenses cannot be deflated but they can be postponed till a later date or the happening of an event wherein they could be explained away without inviting penal action. For example in an investment and financial trading company an amount of Rs 1.8 million was given to a broking house for speculation and investment by a junior fund manager. Somehow the decisions of the junior fund manager went haywire and Rs 1.8 million was lost in speculation and there was nothing left recoverable from the broking house. The fund manager who was responsible for this fund, manipulated and did not record the trades for some months. He was getting desperate, but his patience paid off and luck was on his side. His boss who was the main fund manager was caught in another major scam and that manager absconded. The junior fund manager took his place. The entire Rs. 1.8 million loss was attributed and palmed off to decisions taken by the absconding fund manager and the junior fund manager escaped the wrath of the management for his own misdeeds. Fraudsters are always on the lookout for such opportunities as the sudden departure, death, or other cloaking devices for their own sins. There are two ways to tackle this. One, there has to be an evaluation of accounting discipline; arrears of accounting, updates, reconciliations are clear red flags as also thriving grounds for fraudsters. In fact, all such situations of chaos, disaster (e.g. computer breakdowns, fire, etc.), arrears of accounts, missing records, and sloppy accounting are the hallmarks of an intelligent mastermind of a group of fraudsters, and the most lethal. These are all used to bolster illusionary profits or suppress disaster situations. Secondly any situation of profits not matching reality must be taken with a pinch of salt. For example, huge balances of cash and bank accounts or fixed deposits as against huge over draft balances indicate that in reality the company may not have that much cash. Similarly, huge unexecuted orders for stocks cannot exist logically with huge stocks over re-order levels without any justification of huge pending orders. Another case was in a situation of war, where a hotel was situated close to the enemy territory, there was a sudden increase in profits because of an upsurge in tourism and increase in hotel occupancy just before it was lost by fire for which an insurance claim was received for loss of profits. Such anomalies can be spotted only when the entire business is viewed both on a micro as well as macro basis within the environment. It is not easy, but can be done with a little patience and some research and some clear logical thinking.

As mentioned before, the methods employed by perpetrators of fraud are many and ingenious. However they thrive because of predictable, mundane and standardized methods of review, due diligence and inquiry. Innovative, imaginative and common sense methods can help substantially more in ferreting out such fraud or at least in spotting red flags early.

4. Spotting frauds at a micro level during investigations, audits and risk management exercises.

In order to find frauds at a macro level the forensic accountant looks at fraud risk situations with a bird’s eye view as compared to an ant’s view. A forensic accountant does not look at individual controls for assessing the vulnerabilities but on environmental influences, organization culture, management vision, industry norms and practices and broad policies and guidelines. There can be situations at a macro level, which are conducive for fraudsters. It is possible that such situations can motivate and actually *create* fraudsters. Conversely, fraudsters can also create such situations. In either case, forensic accountants much view these situations as 'red flags' and appropriate modify or extend his audit procedures. The following are some typical fraud prone situations.

5. Situation of disorderliness

Chaos situation, filing indiscipline, arrears in book keeping are usually situations where a perpetrator's actions are not easily traceable. The advantage that a perpetrator has, in such situations, is that he can lead an forensic accountant off-track quite easily. Even if a record or document is available in his drawer, it becomes fairly simple for him to palm it off as untraceable. In most situations, arrears in accounts are a result of fraud rather than non-availability of resources. It may be worthwhile for the forensic accountant to ascertain the responsibility and ownership of the records, the persons who authorized or who have been authorized in the past to have access to these records. It is quite likely that a potential fraudster could be one of these. This red flag when viewed with the other behavioral red flags would give the forensic accountant a better insight into the situation and enable him to identify red flags and eventually detect fraud, if any, existent.

6. Disaster situations

The best camouflage is available to a perpetrator of fraud where some disaster has taken place. For example, where a fire has occurred and its assets and records have been destroyed, it is very simple for an auditee to inflate the inventory of items lost by fire to include fictitious items, items stolen/pilfered in the insurance claim. The convenience of disclosing or not disclosing an available record to the surveyors and investigators is usually exploited by most claimants. Most insurance claims for stocks lost by fire are therefore potential high fraud prone situations. Therefore in large value claims many insurance companies seek help of specialist investigators or accountants to correctly assess the claim.

Example

An interesting case of such a disaster claim happened in a supermarket which was ravaged by vandals during riots. There was a curfew in the city for two days after the riots during which the supermarket remained sealed by the police and un-accessible. On the third day the supermarket presented a situation of complete disaster with stocks strewn all over having been looted by the vandals. Each department manager was sent to his/her department to assess the damage and on the basis of consolidation of all such departmental losses, a huge insurance claim was lodged for loss of stocks and cash. The surveyors got a forensic accountant along with them to take stock of the situation.

To cut a long story short, the forensic accountant found that the cashier had taken advantage of the completely strewn and chaotic condition in the supermarket. The cashier's cabin was in the back office, which actually had not been affected by the riots. But taking advantage of the overall chaos he had vandalized the back office himself. When he entered the cash cubicle he thought that he could conveniently tear and break a few things around to make it appear that the rioters had actually vandalized and stolen cash also. However, he was given away by a simple mistake; he tore some faxes lying on the fax machine, which had been received in the back office **after the riots took place** i.e. during the period when the supermarket had been sealed by the police during the curfew. Therefore since the cashier was the first person entering the cash cubicle after the supermarket was reopened, it was logical that only he could have torn those faxes and on interrogation he confessed. The point worth noting here is that a disaster makes it so simple for any person to commit a wrongdoing that it virtually offers an invitation. Another typical case is a bank robbery. The manager's own embezzlement could be neatly palmed off along with the money stolen by the robbers. Earthquakes, fires, floods or any calamities are situations, where it is possible that a perpetrator could take advantage of palming off past sins or yielding to temptations for new wrongdoings.

7. Organizations left in the 'Autopilot' mode

There is a temple in South India which has a miraculous effect on visitors. The 'prasad' or the divine food offering given to the visitors, tastes delicious only if it is eaten within the precincts of the temple. If the prasad is eaten outside the temple premises, it would taste bland. The symbolic interpretation is that the prasad will retain its divine qualities and taste good only if it is eaten in the presence of the lord. Certain systems and internal controls are like this 'prasad'. They will work well only in the presence of the stake holders or senior management, however robust and well-designed they may otherwise be, and whatever be the strength of built-in internal controls. In other words, when such systems are left on the 'autopilot' mode, they may fail to withstand attacks and contingencies from the external environment. What is this concept of 'autopilot'? Autopilot is a term used to refer to automatic operation of an airplane or a ship without requiring the presence or direct supervision from the pilot or the captain. It is a navigational device that automatically keeps ships, planes or spacecraft on a steady course. While having this autopilot feature has convenience, it can also be devastating if a regular check and supervision is lacking.

Example

This is exactly what happened even when a well-tested, robust computerized application for sales and cash collections accounting was implemented in a bakery, which was left to operate left on the 'autopilot' mode. This bakery had been bought by a company ABCD a few years ago from one of its partners DBP, when he had joined ABCD as a partner in the business. Till it was owned by DBP, it was personally run and supervised by DBP himself. After ABCD had taken over the bakery from DBP the bakery had been left to run under the local manager because there were good time tested systems built in to ensure that it operated satisfactorily. However, the bakery subsequently started making cash losses. These losses of the bakery were attributed to 'drop in sales' due to stiff competition from foreign brands, who even provided free home delivery, and wastage losses resulting in high in-house costs of making breads and pastries. This had resulted in lesser footfalls in the bakery and consequently, lesser sales. The bakery had now come close to going below the break-even point and the management was seriously considering closing the bakery business.

The forensic accountant visited the bakery which was at a far off location. Though the application security and the physical security were indeed good, he realized that they had worked well only as long as they were implemented in the presence of the DBP. His continued physical absence emboldened the local staff to find out ingenious methods of beating the existing level of security. In this case they excused of power outages and the consequent computer-shut downs for resorting to issue of manual cash receipts. The management was told about this in a passing reference and it was led to believe that these were rare occurrences which did not warrant a formal system and such manual receipts were issued only to maintain sales continuity during power breakdowns. On materiality grounds, the management did not think much of these receipts, but ground realities were different. The power outages had become a daily two hour affair which the management did not know, and manual receipts accounted for about 15 % of daily collections which were suppressed and since they were outside the sales system, they were easily embezzled. To justify the drop in sales, the management was led to believe that the sales were falling because of competition and wastage losses

For all its convenience, ‘autopilot’ mode is good for a short duration only and can never be a permanent solution. Permanent autopilot mode can only encourage indifference and fraud on account of perceived safety.

8. Sudden profits in an otherwise loss making business not supported by any reasonable change in environment

It is difficult to believe this, but it may be true that such profits could be illusionary. In fact even if the profits are translated into actual cash receipts they could be misleading. In one such situation the directors argued with the forensic accountant that since the sales proceeds were being regularly received in the banks, how could there be a fraud? The forensic accountant explained that the company’s own capital was being watered. The fraud occurred in a five star hotel on a hill station far away from the nearest city. The hotel had been making continuous losses for years together and the management had decided to close down the hotel and a temporary manager was locally appointed to carry on till the closing formalities were completed. Almost immediately thereafter, amazingly the hotel started making sudden profits, and as the directors argued, the money was being deposited in the bank. However after a detailed investigation it was found that the manager was deceiving the management by clandestinely selling the hotel's own valuable teakwood furniture, expensive glassware and cutlery, paintings, chandeliers and other valuables and depositing a part of the collections in the bank ostensibly as sales, and pocketing the balance himself. What was deposited in the bank as sales thrilled the directors because they really were disillusioned and felt that the new manager had been able to make the hotel turn the corner. To keep his own fraud from being noticed, he would replace expensive valuables like teakwood furniture, cutlery, etc. with ordinary commercial cheap replicas.

9. Consistent losses in an otherwise thriving industry

This needs no explanation and it would be pretty evident to the forensic accountant that losses are not justified. All that the forensic accountant needs to do is to ascertain whether the loss was on account of poor management or intentional mismanagement. This will depend upon exercise of judgment on part of the forensic accountant based on his skills and experience. A fund manager in a derivate trade market which was booming made a huge loss in that period. It was difficult to believe that in such a market a huge loss could be made. It was found that loss was made by entering into large value mindless trades which yielded losses. In reality the purchase and sale of the scrips were deliberately done through two different brokers (which was unnecessary), so that profits equivalent to the losses in the fund manager's company were siphoned out through an intermittent personal broker of the fund manager.

10. Situation of incomplete information: Missing records, seizure of records by authorities, etc.

This is perhaps the strongest red flag of all. An occasional missing document may not be serious but a file or plenty of records missing are certain indicators of fraud in most cases. The missing records usually are so missing with the blessings of superior officers and managers of the organization and would generally indicate a more serious fraud with high level collusion. Similarly in the days of paper records; corrections, white ink changes and alterations were serious issues which would make an forensic accountant prick up his ears.

However, in the paperless environment the focus shifts on user logs and data/program changes. Frequent changes could be symptomatic of foul play.

In a case of an internal audit of vendor empanelment and selection, an forensic accountant observed that the addresses of several vendors were changed and re-changed back to the earlier addresses as per change logs available in the system. These had been done during the floating of the inquiries for certain vendors, to ensure that they did not receive the company's purchase inquiries and therefore would not bid. After the bidding process was over the vendors' master files would be changed back so as to contain the correct addresses. This fraud was noticed when the master file changes were examined for a sample period.

11. Flags at a micro level

These are frauds at the operating level which an forensic accountant comes across while actually carrying out his audit. The seriousness of such red flags is a function of the materiality of the audit area and the overall control environment. If the overall control environment appears to be safe and strong and if the red flag is noticed in a relatively insignificant area then the red flag may not be serious. However it is the forensic accountant's judgment to decide whether to extend his audit check or to ignore the red flag. The following are some of the common red flags within the control environment which an forensic accountant may be watchful of the following.

12. The 'Excess Knowledge' syndrome

There is an incident in the Indian epic 'Ramayana' which is immeasurably important for investigation and interviewing procedures. During the hunt for Sita, some ornaments were found near the place of abduction. When Laxman was asked to identify her ornaments, he could identify only her anklets and none of the other ornaments worn on her person above her feet. Such was Laxman's reverence for Sita and the purity of his mind that his eyes never strayed above her feet. His innocence was clearly evidenced by this ignorance and inability to identify other ornaments. In contrast, guilt would have been indicated by awareness and ability to recognise other ornaments. Thus, during an investigation, the knowledge of any extraordinary fact or information which ordinarily a person is not expected to have, would be a very likely evidence of guilt. Investigations of any financial crime or corruption could be handed over to chartered accountants as a sequel to unusual audit findings or circumstances of suspicion of fraud. This type of red flag is perhaps one of the greatest give away of wrongdoing. A man who knows more than he is supposed to know is likely to have got the information the wrong way. He knows something that he is not supposed to know. For example, a clerk in the purchase department complains about the corrupt practices of his manager and also provides evidence of bills passed at wrong rates or substandard quality materials supplied. It would be essential to understand how that clerk came to know of these matters particularly if they were not relevant to his domain of activities. It would require pretty strong arguments to establish that he got the information accidentally or through some other source innocently.

13. Absence of rotation of duties or prolonged exposure in the same area

For example, where appropriate or sophisticated technical tools for evaluation of quality are not available**,** if there is no system of constant rotation of duties, rotation of suppliers and vendors then the chances of collusion with third parties and within the organization are much greater. Further, if there is complete dependence on external parties the red flag is even more pronounced. If such rotation of duties exists, it should be on a 'surprise basis', and if possible, with new recruits wherever possible. Where identical factories or branches are operating, rotating duties across the branches can bring in much better control and produce phenomenal results. Rotation of duties is a preventive measure which is a must for fraud management.

14. Close nexus with vendors, clients, or external parties

There would be a conflict of interests if an employee, particularly at a senior level, were to have close relations with a client. For example, if a loan officer were to go on a Caribbean cruise with a borrower, it is quite likely that his friendship might come in the way of his duties regarding the loan monitoring obligations. The independence of a person can be evident from the manner in which he behaves with external parties.

15. Gunpowder effect

“Nothing is insignificant until it is proved to be insignificant” is a maxim which is often applicable in many audit situations. As forensic accountants, we often come across situations of control weaknesses of varying intensities. Some of these weaknesses could have serious risk implications while others may not be that serious. While undertaking any risk assessment, forensic accountants tend to concentrate on the serious risk implications and usually do not give more than a casual look to the trivial and smaller weaknesses and control deficiencies. This is a reasonable method of assessing the overall risk. However, there are exceptional situations, where these seemingly small control weaknesses may certainly be insignificant individually but collectively pose a greater threat. To understand this, take some commonplace kitchen items, such as charcoal, salt petre and Sulphur. In the olden days, these were routinely used in Chinese kitchens, for harmless cooking purposes. Saltpetre or potassium nitrate was used in cooking meat, charcoal was used as fuel, and Sulphur was used as a substance to intensify the heat. The point to be noted is that, individually they were relatively harmless and in fact useful, but combined together, they formed a dangerous explosive substance: gunpowder which is used not in kitchens but in battlefields. This is what forensic accountants need to be mindful of in audit situations.

Seemingly unimportant control risks could be individually harmless and perhaps useful in the ordinary course of business, but collectively, they could become a major risk factor. In normal audit situations, such control weaknesses may be spread over and easily hidden among myriad procedures. The forensic accountant may have to spend some time weeding out those which are genuinely harmless and shortlist those which could be dangerous collectively that is, those who could inflict a kind of a gunpowder effect. The point to be noted is that control weaknesses may appear small or not so serious. The forensic accountant should not make the mistake of viewing them in isolation. Study all the audit observations from a distance as well as from close quarters. This will enable a macro-micro view and facilitate forming an opinion.

Example

During a risk assessment of a trading business firm an forensic accountant was going through the list of observations where he found a small paragraph captioned as ‘Other miscellaneous observations’. The observations included miscellaneous issues such as “Practice of leaving blank signed cheques, non-insistence of the firm to obtain receipts for payments to parties, several stale cheques not reversed in the books of account”. Individually all these three observations did not appear malicious nor severely harmful to the company, but collectively, they inflicted the explosive gunpowder effect. They facilitated the accountant to perpetrate the fraud as follows:

The accountant would intentionally keep some ‘emergency’ payments for creditors, LIC PPF, etc. on standby, when the partners were travelling. This would make it necessary for the partners to sign some blank cheques to be used while they were away. Some of these blank cheques would be intelligently used for genuine purposes and shown accordingly in the cheque counterfoils. One or two of these cheques would use for a fraudulent purpose and explained away as cancelled cheques, or as cheques lying somewhere in the cash box, which the partners never bothered to physically verify. When the partners were away he would use those blank signed cheques, to redivert payments to LIC, or PPF (or any payment where no immediate backlash was expected for non-payment), to his personal account. Since this re-diversion had to be done at a convenient and opportune time, there was a camouflage required, which was achieved by allowing cheques to remain unpresented. Therefore stale cheques appearing in the bank reconciliation statement at all times could not be helped, but he did not reverse them deliberately even after six months. The actual cheques issued to LIC, etc. were torn and thrown away. The lapsed LIC policies, or the PPF account balances were not shown to the partners who usually did not bother about these at all, till this fraud was exposed.

The point to be noted is that several small irritants could snowball into a big issue; therefore it is advisable never to discard any observation as harmless unless and until it is so proved conclusively.

16. Sudden Losses

While sudden profits are to be reviewed from a macro level and compared with industry conditions, losses should be viewed within a company and root cause analysis needs to be carried out. The forensic accountant must be able to distinguish between a genuine business loss or adroit manipulation of revenues for ulterior motives.

Suppose a company doing quite well suddenly makes huge losses**.** While there could be genuine reasons, mismanagement of funds and resources are more likely. It is possible that these losses had been there all along simmering under window dressed accounts. Once the bubble bursts, however the losses erupt and it appears as though sudden losses have hit the business. The genesis of the losses could have been siphoning of funds, inflation of expense or suppression of income or a combination of all.

17. TGTBT syndrome "TGTBT" stands for "Too Good To Be True"

Lovely glossy reports may be furnished whereas in real terms there may be gloomy conditions. In the sudden profits' illustration given earlier the hotel results actually showed a turnaround of the losses into fantastic profits, which were actually nothing but proceeds of clandestinely sold fixed assets. Effectively the hotel was rapidly watering down its capital and the fraudster was helping himself in the bargain. What is also learnt, from this example, is the truth of the proverb ***"all that glitters is not gold"***.

Example

In a particular case, a supplier in a ghee producing plant agreed to supply milk at extremely low rates which none of the competitors could afford. Strangely the supplier stoically also bore the cost of heavy rejection of milk supplied by him by the company's quality control department. The rejections amounted to one third of the total supplies. Thus where he was supplying milk worth INR 220 million annually, in real terms he had delivered INR 330 million worth of milk of which INR 110 million was taken back as rejection. The company got INR 220 million of milk at an extremely low rate which was **too good to be true**. Practically, the forensic accountant wondered, what could he be doing with INR 110 million of rejected milk?

The investigation revealed that the supplier was indulging in ***piggyback tanker fraud*** wherein two tankers came in simultaneously to deliver milk, out of which one truck carried substandard milk. While the quality control department was testing the sample, the number plates of the tankers were switched so that the tanker carrying the good milk returned as rejected milk and the substandard milk was offloaded as good milk. The tanker containing the good milk would then be sent back a few hours later which obviously would be cleared for taken out of the company premises by the quality control (considering this to be the substandard milk). Thus, the supplier could supply milk at very low rates which were affordable to him, because in reality he was deceiving the company regarding the quality for 50% of the milk delivered and the company paid for substandard milk without realizing it.

Example

Another TGTBT illustration was the case of an EDP manager, who appeared to be a very dedicated man. He would be the first to enter the office and usually the last to leave. He was highly respected and admired for his dedication and hard work. But an investigation later revealed, that he was involved in manipulating data and certain in-house applications for receivables and payables to transfer credits to certain favored parties. In fact, he was manipulating his own loan account to show 'nil' overdue even though he had not paid for several months. The point here is; what appears to be good needs to be tested before accepting the true value. In the section relating to case studies for forensic accountant, there is a very interesting case study of a change in the behavior of a fund manager. Generally known to be sloppy and indifferent in his attitude to work, one fine day this fund manager suddenly became very concerned about reconciliations and actually found out an error which got the company INR 4.5 million. This was a typically unbelievable TGTBT syndrome and actually was a fraud.

18. Existence of 'orphan' funds

Orphan funds are funds which are available to a person/group who are not disciplinarily accountable for their usage. Funds which are held in a fiduciary capacity such as funds collected by trusts or donations in cash collection boxes are typical examples where there is no accountability for their usage. Donors believe that funds will be used for noble purposes and they seldom concern themselves about the usage of the funds. On the other hand, the intended beneficiary does not make a direct claim for such funds because he has no control and in many cases, he does not even know of the existence of such funds collected for him. Such funds can sometimes be substantial and virtually invite perpetrators to commit fraud. This analogy of orphan funds can be applied to funds given to consultant companies for project governance. Even in advertising companies, they are given pre-approved budgets for production jobs. Economies of scale in such companies are exploited at the client's expense since the client does not know about them and does not protest as long as the budgets are not overrun. The management of the advertising company also does not bother as long as the client does not raise a squawk because the funds spent are the clients funds over which the client has lost interest, thus they are 'orphan funds'.

To explain this with an example, suppose an advertising company uses the services of translators and other freelance services. The client will usually pay whatever the advertising company spends within the budget approved in advance, and depend upon its honesty. The advertising company itself will also make inquiries with norms and industry standards and quote rates for such payments and propose budgets accordingly. However the actual disbursements do not necessarily match such budgets and do not reach in full to the intended payees as desired. In a very shrewd manipulation, in such a scenario, a fraudster saw a wonderful opportunity of using certain budgeted 'orphan' funds for translation jobs. Translators' fees were payable slab-wise for 100 words for any language. The fraudster would allocate and consolidate several different clients' jobs in the same so that they would be just below the 100 word limit and therefore he would pay only one translator. However he would claim a separate reimbursement for payments made to several translators for each of the clients' jobs. The clients would willingly approve the individual payments since these were within the budgets little knowing that the actual cost had been split over several clients. The management of the advertising was blissfully unaware and probably did not care because the 'orphan' funds did not belong to the advertising company. Since the advertising company would be given funds for each job separately it could legitimately use funds made available by the client/s (see ¶5-020).

Thus in orphan funds, often the intended beneficiaries do not get the funds and the entities providing these funds are not aware of the economies of scale and benefits available at the grass root level. This analogy can also be typically misused when huge funds are placed with contractors, project consultants, etc., for purchase of materials, services etc. Cranes hired could be used for several other projects during idle time. Revenues generated are never reported to the rightful owners/hirers of the cranes. Thus, such situations where funds are lavishly available for use which is not easy to monitor are the places where any forensic accountant/investigator must look into first.

19. Irrational behavior

Behavior which is not becoming of the employees' position and which does not keep in mind the decorum of an office often, stems from deep rooted insecurity which could be symptomatic of fraudulent intentions. For example, a person who is always rude and inconsiderate, or overly secretive, is likely to be behaving in that way to suppress fraud or some kind of deceitful act. The intention is keep others at bay so as to avoid inadvertently revealing guilt or to cover some malafide act. The seven Cardinal Sins identified in the Bible, include 'sloth' as one of the cardinal sins. Compared to the other sins, sloth on first count does not seem to be that devious or evil a trait. However, a little reflection will enable a forensic accountant to realize when sloth can be a symptom of mala fide intentions and deeds.

In a supermarket on a highway far away from a metro city there was a cashier to whom the entire supermarket was entrusted by the owners. The owner had full faith in his integrity and honesty and in a discussion with the forensic accountant once remarked that, but for his slow manner of working he was an asset and that, he had no fear of any kind of fraud or deceit on the part of the cashier. In order to satisfy himself the forensic accountant went to see the supermarket himself and he was surprised to see that the cash collection was a simple process of tallying the day's total collections with the system's cash balance and for a person who had been on the counter for 20 odd years this should have been a cinch. There was absolutely no reason for him to take an extraordinarily long time to carry out this task. The forensic accountant kept him under surveillance and eventually found that he was selling certain imported smuggled items (cigarettes, lighters, perfumes, toiletries) clandestinely for which he had to monitor total collection at the end of the day. That was the reason for taking so much time in tallying cash balance since he had to segregate his own clandestine sales from the owner's official sales. Thus sloth in situations where speed is expected naturally can be symptomatic of fraud.

Thus red flags are important and inevitable in any audit as well as fraud detection/investigation assignment. It is believed that majority of the frauds that are discovered are certainly not by forensic accountants and a very small percentage of frauds are actually discovered during audits. Those that are discovered are chance discoveries where forensic accountants have 'stumbled' on to these frauds while doing something else. Frauds are rarely discovered with the help of strategically planned procedures.

Therefore to improve chances of fraud detection the ability to spot red flags is the key issue. The foregoing is certainly not an exhaustive list of red flags and this list can keep on extending to include new red flags seen by forensic accountants. Fraudsters will always continue to find newer techniques and methods of weaving their webs of deceit.

Chapter 2: **Case Studies on business fraud- 'distrust the obvious' and the green flag syndrome**

We have heard of red flags which are symptoms or indicators of fraud, white collar crime or something detrimental to an entity's interest. For example, shortages in stocks, close nexus with third parties, missing documents or missing cheques, shortage in collection, etc. are all signals indicating that something is amiss. Such signals, if and when noticed, automatically raise alarm bells and imply the possibility of fraud in some form are called red flags. However there are other signals which could also imply the existence of fraud *but such signals do not activate alarm bells*. On the contrary they may even lead to a greater sense of assurance and comfort in a scenario which may be potentially infused with fraud. These signals could be called as 'green flags'. The only thing which identifies them is that they are unusual signs or oddities or inconsistencies, but apparently harmless or perhaps even helpful

1. **Unidirectional errors- e.g. excess cash but never any shortage**: In a unique case there was a cashiers showed always showed excess cash on cash counts, never any shortages.

2. **An otherwise sloppy accountant suddenly turns very responsible** and initiates a reconciliation of an amount receivable from a consignee for the past three years. This amazingly bears fruit and some money is actually received for an item sold in the previous year by that consignee, but not reported by him in that year. This accountant did not even know how to do a proper bank reconciliation, but the directors rewarded him.

3. **Self-inflicted punishment**: An accountant/ employee pays from his own pocket to make up for a double payment 'inadvertently' approved and paid by him.

4. Sales and Service station jobs statistically moved together in a service station and sales outlet of a TV manufacturing company.

5. **Unexpected windfall income in certain situations**. There were certain unidentified cheques received at the head office by a branded educational institution who organized specialized and popular training workshops and seminars all over India, particularly rural areas. Most such cheques were received by courier or post without any details or at best a covering letter from

reputed companies stating that the cheque was sent for participation by its employees in training workshops conducted by the Institution.

6. **Overly strict disciplinarian QC manager**: Extremely harsh behavior of QC manager in rejecting food biscuits manufactured by a subcontractor. Rejections to the tune of almost twice the production. The subcontractor was penalized the raw material cost for the rejection. Thus he almost lost more than 3 quarters of his profit in the penalty for rejections. Similarly in factories, there are QC managers who implement a very strict policy of heavy rejection of stores, spares and equipment in factory. This was observed even in a soyabean purchase plant

7. **Employee did not take advances**/ cash float when he goes on outstation tours for company purposes. He spends from his own funds and presents travel bills almost two years later. Explanation- excessive touring and return to home town for very short periods which did not leave him time to prepare expense details. These piled up.

Chapter 3. **Introduction to mathematical and quantitative techniques for investigation**

The forensic accountant would be severely handicapped without knowledge and experience of mathematical techniques of investigation. In modern times and times yet to come use of manual techniques for data analysis is virtually out of question. The ability to discern quality of data, its reliability, latent trends and to carry out meaningful analysis such as classification, sorting, summarization in myriad ways to meet the needs of a given situation is absolutely essential. The forensic accountant therefore needs some expertise in use of mathematics, statistics and above all imaginative thinking. Only if he possesses these capabilities will he be able to query data in the most appropriate and kaleidoscopic manner to get meaningful results.

Generally the following are the different methods applied for carrying out investigations:

1. Relative Size factor
2. Benford's Theorem
3. Data mining using either audit software or even spreadsheets such as MS Excel, it is possible to ferret out missing document numbers such as missing cheques, receipts, dispatch notes or duplicated invoices etc. Data can also be sorted, classified, stratified in multiple ways to understand the trends more penetrative.

A very detailed note on use of excel in investigations is given along with in this hand book and demonstrations with case studies for data mining is given in Chapter 6

The Relative Size Factor and Benford's theorem are explained below.

Relative Size Factor (RSF)

Relevance :

Scrutiny of individual parties account is humanly ineffective and now with most of the data available digitally how does one scrutinize the ledgers? RSF theory comes in very handy here, instantly one can calculate RSF and take sample for verification. This tool finds focus and meaning to the scrutiny. It highlights all unusual fluctuations which may be stemming from frauds or errors.

What is RSF ?

- RSF is the ratio of Largest Number to the Second Largest Number of a relevant set.

$$\text{RSF} = \frac{\text{Largest Number}}{\text{Second Largest Number}}$$

For example, if we have following bank payment vouchers of Vendor XYZ

Voucher No.	Rs.
SB-211	50,000
SB-642	5,00,000
SB-547	5,00,000
SB-1864	20,000
SB-4755	23,000
SB-8347	8,500

The Largest value in above table = Rs 5,00,000/- and the second largest value = Rs 50,000/-. Therefore the RSF in this case = 10 that is Rs 5,00,000 Lacs divided by Rs. 50,000/-

Application of RSF theory in audit

- Any set of transactions generally take place in certain range or limits. Thus there is a certain pattern of financial limits peculiar to each vendor, customer, employee, etc. These limits may not be defined, but the data can be analyzed to view a pattern. RSF captures this pattern as ratio.
- For example in case of vendor X the normal invoicing range, say is Rs. 20k to 50k per bill. If there is any stray instance of single transaction which is way beyond the normal range than that ought to be looked into. That is, in the instant case, if there is bill of Rs. 5 lacs than it naturally concerns the auditor to have a look at.
- RSF is above case will give a ratio of 10. That is. ratio of Rs. 5lacs (largest value) to Rs. 0.50 lacs(second largest value)
- This single instance could be case where there is some foul play or error in punching of the data (due to additional zero at the end).

Case study on use of RSF using Excel Spread Sheet

ICE, a large multinational white goods company had set up operations in India in the year 2000 by acquiring a small local manufacturing company and expanded its operations country-wide. The investigators were called in the year 2003 / 2004 pursuant to allegations contained in an anonymous letter against the Plant Manager. Initial engagement discussion revealed that the ICE's outflows mainly comprised of labour payments, power, capex, raw materials, job-works, R&M, etc.

The investigator first ran a check of RSF on the vendor data and got the following parties where the RSF exceeded 10.

Vendor	**Max_Val**	**2nd Max_Val**	**RSF > 10**
WAP Systems LLC	25,748,906	2,059,912	12.50
Indergoll Rand Ltd	206,788,550	13,586,007	15.22
Difel Inc.	96,574,432	3,094,148	31.21
Ajmera Constructions	45,659,440	1,551,753	29.42
A-Technologies Ltd	13,478,523	705,870	19.09

A drill-down on the voucher level details of the above vendors revealed following information

Name	Doc Ref	Date	Rs.	Particulars	No. Of Cases
WAP Sys	17089343	31-Mar-01	25,748,906	WAP –ERP System Capitalised	14
WAP Sys	18088874	06-May-02	2,059,912	WAP-system-AMC for 2 years	14
Indergoll	17089352	31-Mar-01	206,788,550	SW, PS, Asly-line Capitalised	22
Indergoll	17089353	31-Mar-01	13,586,007	P&M Erection and Comm.Chgs	22
Difel	17089355	31-Mar-01	96,574,432	Foaming System Capitalised	16
Difel	18089983	05-Jun-01	3,094,148	Foaming cryst s/w capitalised	16
Ajmera	17069323	15-Jan-01	45,659,440	FacBldg., Admr Wing, Stores, FGStore	18
Ajmera	17070222	02-Feb-01	1,551,753	Interiors-Office, Mng., Conf., Canteen	18
A-Techn	37852344	25-Mar-03	13,478,523	Mould qty1 -SKE 4011Stellar	4,586
A-Techn	18088874	21-Jan-03	705,870	Mould Job wrk HDL-5004 - 15000 nos.	4,586

Considering the information obtained, the RSF of M/s. WAP, Indergoll, Difel, Ajmera were explainable since they had basically supplied capital items which was one time large cost and subsequent bills would be for supply of services/

spares etc. and hence the cost would be much lower. However, A-Tech was a job worker and had issued over 4,500 bills. So the pattern of his general transactions were in range of 50,000 to 7,00,000/-, thus the off-beat transaction of Rs 1.34 Crores needed a review.

The investigator made inquiries of the transaction for Rs. 1.34 Cr and learnt that it was towards the cost of mould purchased from A-Tech. General review of accounting documents and supporting showed everything to be in order. He was explained that generally moulds are procured from another vendor but this one was purchased since ATech was L1. The investigator reviewed the quotes received, bid comparison, etc. and noted that indeed A-tech was lowest. He also noted that the next bid value was about Rs 3 Crs that is more than double then the quote of A-Tech. This raised a red-flag that how was A-Tech able to supply the same mould in less than half of its competitor. He decided to inspect the asset. To cut the long story short, when he investigated into the procurement, it was found that the mould actually belonged to the ICE only which was not in use and had been discarded by the previous management of ICE and later sold as scrap to A-tech. The plant manager in connivance with the A-tech created the need for a mould which was little bit modified and put to use. The mould was however sold back to the company at much higher profit.

How to calculate RSF in MS Excel

Given data of about 1000 records extracted from Account payable system. The data consists of foll. relevant fields.

- ✓ Voucher No.
- ✓ Voucher Date
- ✓ Vendor Name
- ✓ Bill Amount
- ✓ Bill Number

The objective is to find out the RSF for each vendor in following format

Vendor	Max_Val	2nd Max_Val	RSF
Col _A	**Col_B**	**Col_C**	**Col_D**

Summarized Steps

Step 1 : Extract the maximum value for each vendor and store in a column of the work sheet – say col. B

Step 2 : Extract the second maximum value for each vendor and store in another column say col. C

Step 3 : Divide Col. 'B' by 'C' to get RSF Ratio and store result in Col. 'D'

Step 4 :Filter Col. 'D' for results where RSF is more than say 10.

Step 5 : Filter records from Database for the above results as audit sample.

Detailed Steps

Step 1 : To obtain the largest or maximum value from the data

- Use Pivot Table Function to classify the bill-amount field of data.
- The classification criteria will be vendor name
- Classification of Bill amount field will be for "Max. Value"

Step 2 : To obtain the 2nd maximum value from the data

- To obtain the 2nd max value, it will be necessary to nullify the max. values obtained in Step 1 above. This can be done as follows.
- Extract results obtain from the first step to append to the data with the maximum value for the each respective vendor. This can be done by using 'Vlookup' Function.

  Formula = Vlookup(CriteriaCellRef, DataSource, Offset)

- Nullify the effect of the bill amount if the respective bill value is equal to the Max. value. Using the ‘If’ function.

  Formula = If(BillValueCellRef = MaxValueCellRef, 0, BillValueCellRef.)

  [The above formula will add to the existing database, a field with bill amount which is not a MAX.Value.]
- Repeat The First Step again to obtain the max value from the field created above. The max value now will be actually the 2nd Max. value.

Step 3 : Divide the Max Value with 2nd max Value

- This is a simple divide function

$$\text{Formula} = \frac{\text{MaxValueCellRef}}{\text{2nd MaxValueCellRef}}$$

- The result obtained is RSF

Step 4 : Filter the RSF col. to extract where RSF is more than say 10

- This can be done using the Auto Filter Command of excel sheet by customizing the limits.
- The result obtained are data where RSF is more than 10.

Step 5 : Filter records from Database for the above results.

- This is same as filter command used in Step 4, except that now the filter is set on the main database.
- This data is records where the max value of bills exceeded the 2nd max value over five times.

Benford's Law Theorem

Backdrop, concept and objective.

There is a story which nicely encapsulates the objective of Benford's theorem.

Somewhere in the USA, a professor, asks his mathematics students to do a homework assignment: Flip a coin 200 times and record the results of heads or tails and submit their papers to him the next day. The following day, on receiving the papers he runs his eye over the homework data, and to the students' amazement, he easily spots all those who faked their results of the tosses. The truth is that most people don't know the real odds of such an exercise, so they can't fake data convincingly. The overwhelming odds are that, at some point in a series of 200 tosses, either heads or tails will come up six or more times *in a row*. Most fakers don't know this and avoid guessing long runs of heads or tails, which they mistakenly believe to be improbable. Therefore, at just a glance, the professor could see whether or not a student's 200 coin-toss results contained a run of six heads or tails; if they didn't, the student had probably faked the results. However, there is more to this than merely a classroom trick. *Data validation is the underlying objective of an astonishing mathematical theorem known as Benford's Law*. This is a powerful and relatively simple tool for pointing suspicion at frauds, embezzlers, tax evaders, sloppy accountants and even computer bugs.

Benford's Law is named after the late Dr. Frank Benford, a physicist at the General Electric Company. In 1938, he noticed that pages of logarithms corresponding to numbers starting with the numeral 1 were much dirtier and more worn than other pages. When he saw that the top pages (relating to smaller numbers 1,2, 3) of the logarithmic books were used more, Dr. Benford concluded that it was unlikely that physicists and engineers had some special preference for logarithms starting with smaller numbers like 1, 2 or 3. There had to be some reason. He wanted to understand and analyze this peculiarity. He embarked on a mathematical analysis of 20,229 sets of numbers, including such wildly disparate categories as the areas of rivers, baseball statistics, numbers in magazine articles and the street addresses of the first 342 people listed in the book "American Men of Science." All these seemingly unrelated sets of numbers followed the same first-digit probability pattern as the worn pages of logarithm tables suggested. In all cases, the number 1 turned up as the first digit about 30 percent of the time, more often than any other. After analyzing several sets of naturally occurring data a new pattern of digits' appearance was discovered, what later became Benford's law which can be simply explained as follows:

When the logarithms of the digits 1 through 9 are plotted they look like the number line shown below:

Logarithmic Table:

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
30.1%	17.6%	12.5%	9.7%	7.9%	6.7%	5.8%	5.1%	4.6%

Thus in simple words this law defies the normal law of probability which would state that every digit has an equal chance of appearing. To understand this law take a simple illustration. If one were to be examining 1000 cheque payments, by the law of probability payments beginning with the digit 1 (e.g. Rs. 1,200 or Rs 1,23,000 or Rs 17 etc.) would have as much chance as payments beginning with the digit 2 (e.g. Rs23, Rs23,987, or Rs 2) or as any digit from 1 to 9. Accordingly it can be deduced that each digit has a 1/9 or 11.1 % chance of appearing and thus the normal law of probability would mean and imply that payments beginning with one should be 11.1 % of the 1000 cheque payments that are being examined as also those beginning with 2,3 … up to 9. This is where Dr Benford differs. He states that the payments beginning with the digit 1 would be 30.1 % and NOT 11.1 % and the table above is what is the expected appearance of cheque amounts beginning with 2,3…upto 9 respectively. This is what Benford claims and he further states that any natural number population which does not confirm to this pattern, within tolerable limits (defined by using the statistical Z test), then there is some artificial influence of error or fraud and the data is not reliable where the percentages have overruns.

(Actually, this rather amazing fact was discovered in 1881 by the American astronomer Simon Newcomb. Pocket calculators were not even a dream at that time. Calculations were made using pencil and paper. Books with page after page of logarithm tables were used for complex calculations. Newcomb noticed that the pages of the logarithm books containing numbers starting with 1 were much more worn than the other pages. Unfortunately, Newcomb was rewarded for his effort by being ignored. In 1938 Dr. Frank Benford studied the same thing with a much larger amount of data than Newcomb. Unlike Newcomb, Benford was recognized for his contributions and the relationship he derived was eventually named Benford's law in his honor).

General Features of Benford’s Law

Benford's law has been used as a method for spotting fraudulent accounting data by looking at the first significant digit of each data entry and comparing the actual frequency of occurrence with the predicted frequency. Most white collar criminals are unaware of Benford's law and will use each digit about 10% of the time for the first significant digit in a number.

Benford's law doesn't work for numbers controlled to a specific value, nor does it work for truly random numbers such as those generated by a random number generator.

Benford's law also doesn't work well for small sample sizes. However, it holds true in a surprising number of situations. The larger and more varied the sampling of numbers from different data sets, mathematicians have found, the more closely the distribution of numbers approaches what Benford's Law predicted.

Benford's law shows that natural processes can be remarkably resistant to complete randomness.

A strange feature of these probabilities is that they are "scale invariant" and "base invariant." For example, it doesn't matter whether the numbers are based on the dollar prices of stocks or their prices in yen or marks, nor does it matter if the numbers are translated from one currency to another. A Benford’s set will remain a Benford’s set.

Caution:

But Benford’s Law doesn’t apply everywhere nor is it in fallible. It applies only to natural number populations First, you need to have a big enough sample size so that patterns can show themselves. For example, you almost certainly won’t find Benford’s Law in the heights of your average family of 4.5 people. Second, you don’t want numbers that are truly random. By definition, in a random number, every digit from 0 to 9 has an equal chance of appearing in any position in that number.

And third, you don’t want numbers that are the complete opposite of random, and are tightly controlled.

In what way would Benford's Theorem be useful to Auditors?

Benford's theorem offers a number of possibilities. The numbers that appear in accountancy tables, and the balance sheets of companies, follow Benford's Law. This was discovered by Dr. Mark Nigrini, in his Ph. D. thesis written in 1992. However this law can be used for more specific audit purposes.

Overview of data.

Essentially this theorem provides a tool for data validation. Therefore the first use of this tool can be to get an overview of the audit data. If the data is plotted and analyzed using this tool an auditor can, with a reasonable assurance, conclude whether there is any material artificial influence either by way of fraud or error on the data. For example, if an auditor is analyzing say 1,00,000 cheque payments and using digital tools he is able to segregate the data as follows:

Cheque amounts beginning with the digit	Actual	%	Benford's %	Variance %
1	328	35.12	30.10	5.01
2	173	18.52	17.61	0.91
3	110	11.78	12.49	-0.72
4	89	9.53	9.69	-0.16
5	83	8.89	7.92	0.97
6	59	6.32	6.70	-0.38
7	34	3.64	5.80	-2.16
8	26	2.78	5.12	-2.33
9	32	3.42	4.57	-1.14
Total	**934**	**100**	**100**	

Audit Sampling.

The auditor can further direct his attention to that part of the audit population where he feels that the actual distribution of the data is not conforming strictly to this theorem. The test of Benford's theorem is done using tolerance limits provided by the 'Z' factor test. The Z factor test details are available in any book on statistics and probability and is easy to implement using digital tools. For example in the above instance if the data had shown the following variance, he would have examined all transactions beginning with the shaded below, where there is an overrun. In simple words, the law helps an auditor to focus his attention to areas where some error or fraud is likely.

Cheque amounts beginning with the digit	Actual	%	Benford's %	Tolerance Z factor test %	Variance %
1	328	35.12	30.10	3.31	5.01
2	173	18.52	17.61	0.69	0.91
3	110	11.78	12.49	0.61	-0.72
4	89	9.53	9.69	0.11	-0.16
5	83	8.89	7.92	1.04	0.97
6	59	6.32	6.70	0.40	-0.38
7	34	3.64	5.80	2.75	-2.16
8	26	2.78	5.12	3.16	-2.33
9	32	3.42	4.57	1.60	-1.14
Total	**934**	**100**	**100**		

Detection of fraud and errors.

At an advanced stage when this theorem is used more intensively, the auditor can perhaps develop models and algorithms to detect frauds and errors. The foregoing discussion of this theorem has just touched upon the elementary aspects of Benford's Law. However this law not only talks of appearance of the first digit but also gives predictions of appearance of round numbers, second digit, third digit, first and second digit, first second and third digits and so on. It would be too lengthy to explain each type of prediction but those auditors who are interested may study and understand this theorem and its corollaries minutely to be able to apply it intensively in their audit.

Kind of frauds or errors which can be exposed using Benford's Theorem, not being one off isolated instances:

Since the theorem places a lot of importance on the natural appearance of digits and patterns of numbers any deliberate or even unintentional acts which lead to changes in audit populations would be highlighted by applying this theorem. Of course this would be exposed only if such acts are regular and material and not applicable to occasional isolated acts. For example if a particular manager is liberal in approving expense bills but his authority is restricted to say Rs5,000 most employees would try and keep their expense bills below Rs 5,000 and therefore there would be an overrun of expenses between 4,000 and 5,000 and therefore the Benford's theorem would show that there are more transactions beginning with 4 than those as per his prediction. In such cases an auditor would want to audit all transactions beginning with the digit 4. Thus applying Benford's theorem, (for the first digit appearance) it may be possible for an auditor to detect frauds/errors of the following type:

1. Too many vouchers below a certain authority limit
2. Regularly duplicated/replicated amounts
3. Alterations and manipulations in accounts
4. Coding errors, data entry errors, or sloppy accounting practices affecting financial statements

Situations where an auditor can use this law

This law can be used virtually in any audit population such as sales, purchases, inventory, payments, receipts, etc. where there is no limit or any specific artificial influence such as sequential control. Benford's law is increasingly used in the accounts payable area to detect broken payments of just under limit approvals. In one particular case when the auditor plotted the actual occurrences of the first two digits in the accounts payable database as against the expected frequencies benchmarked by Benford, he could immediately identify unreasonably large number of transactions beginning with the digit 79. On a closer examination of these records, it surfaced that most of these payments were broken payments pertaining to invoices which far exceeded the authorization limit of a particular accounts payable manager. The invoices were broken up in amounts that were just below the authorization limit fixed for that manager.

Technical aspects:

For those who wish to understand the technical aspects of this theorem, Dr. Benford derived a formula to explain this law. If absolute certainty is defined as 1 and absolute impossibility as 0, then the probability of any number "d" from 1 through 9 being the first digit is log to the base 10 of (1 + 1/d). This formula predicts the frequencies of numbers found in many categories of statistics.

(A logarithm is an exponent. Any number can be expressed as the fractional exponent -- the logarithm -- of some base number, such as 10. Published tables permit users to look up logarithms corresponding to numbers, or numbers corresponding to logarithms. Logarithm tables (and the slide rules derived from them) are not much used for routine calculating anymore; electronic calculators and computers are simpler and faster. But logarithms remain important in many scientific and technical applications, and they were a key element in Dr. Benford's discovery.)

When the logarithms of the digits 1 through 9 are plotted they look like the number line shown below:

Logarithmic Table:

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
30.1%	17.6%	12.5%	9.7%	7.9%	6.7%	5.8%	5.1%	4.6%

This means that all numbers starting with a "1" will occupy 30.1% of the total length of the scale. Numbers like 1.23784, 1.5, or 1.879 would fall in this region.

Note that these relative distances are independent of the power of ten a number is multiplied by. For example, the distance between .001 and .002 on a logarithmic scale is identical to the distance between 1000 and 2000. In other words the distance between 1 x 10^{-3} and 2 x 10^{-3} is identical to the distance between 1 x 10^{3} and 2 x 10^{3}. Again the power of ten makes no difference on a logarithmic scale.

Zeros are also not considered as first significant digits in a decimal fraction because they are only used as place holders to indicate the location of the decimal point. For example, .001 would be written as 1 x 10^{3}. One would be considered the first significant digit.

Benford reasoned that the length of the distance from one number to the next divided by the length of the entire scale would give the probability of the digit being the first one in a given data value. Mathematically this is expressed as follows for base 10 numbers:

$$P = \frac{\text{Log}_{10}(n+1) - \text{Log}_{10} n}{\text{Log}_{10} 10 - \text{Log}_{10} 1}$$

$$= \text{Log}_{10}(n+1) - \text{Log}_{10} n$$

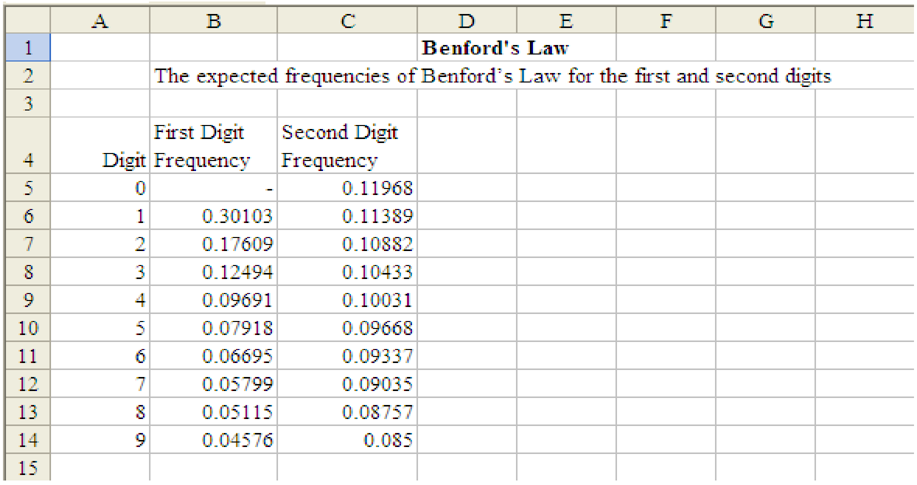
$$= \text{Log}_{10}(1+1/n)$$

where: n = the first significant digit of a number

Notice that if a data entry (base 10) begins with a 1, the entry has to be at most doubled to have a first significant digit of 2. However, if a data entry begins with a 9, it only has to be increased by, at most, 11% to change the first significant digit into a 1. This once again illustrates that a first significant digit of 1 is more likely to occur than a 9.

Applying Benford's Law:

The expected probability of numbers as first and second digits as discovered by Benford is tabulated below. See Figure



	A	B	C	D	E	F	G	H
1				**Benford's Law**				
2		The expected frequencies of Benford's Law for the first and second digits						
3								
4	Digit	First Digit Frequency	Second Digit Frequency					
5	0	-	0.11968					
6	1	0.30103	0.11389					
7	2	0.17609	0.10882					
8	3	0.12494	0.10433					
9	4	0.09691	0.10031					
10	5	0.07918	0.09668					
11	6	0.06695	0.09337					
12	7	0.05799	0.09035					
13	8	0.05115	0.08757					
14	9	0.04576	0.085					
15								

Case study using Benford's Law:

An auditor who tried out this test using audit software in an engineering company on a population data comprising of cheque payments for the entire company running into a volume of about 3000 transactions for a quarter. This test was independently conducted by someone different from the audit team. The results were amazing. The actual frequencies matched quite closely with the Benford's expected frequency distribution as given in the table. Absence of deviations were corroborated by the findings of the routine audit team which did not reveal any material discrepancy from the sample check carried out. The fact that the percentages of appearance of leftmost digits matched Benford's predictions cannot be a mere coincidence and it was reasonable to support Benford's theory that there was very little chance of contamination of that population by way of fraud or error.

However, the above is a positive test and may not be convincing enough. What is really important is also to know whether this works where there is an error or fraud. The following example is one which illustrates the negative findings, which eventually revealed a fraud cleverly perpetrated.

In a large and popular restaurant, there was a lunch buffet priced at Rs.100/- per person. Normally there would be a waiting period to get a place even though there were a large number of tables and covers. An auditor applied the digital test on cash memo collections for a period under audit. He was surprised to find that the cash memo collection amounts for that period beginning with the digit '1', (for example cash memos for Rs.100/- from single customers or cash memos for Rs.1000/- for 10 customers, or Rs.1100/- for 11 and so on) were only 18% whereas Benford's Law states that they should have been 30.1%. The auditor attempted to get more information regarding collections from the local manager and he got some useful data from him. He learnt that a large part of their patronage was from single customers who were executives from the nearby corporate offices who came for lunch, mostly alone. They were quite regular and therefore cash memos for single customer lunches (Rs.100/-) should have been substantial and at least Benford's theorem relating to the digit 1 seemed to be true and applicable. Carrying out his analysis further, the auditor filtered out data relating to single customer cash memos (Rs.100/- cash memos) and averaged them for a month. He found that the average single customer cash memo collection per day did not exceed Rs.1500/- *i.e.* not more than 15 such single customers had lunch in a day. However, the manager said that this was not correct because at least 25 such single customers patronized the restaurant each day. Even the auditor confirmed this when he personally visited the restaurant the next day at lunch time. He also concluded that there could not be loss of revenue by customers walking away without paying since no customer could get a table unless he had paid his money in advance and collected a computerized cash memo. The only other possibility that remained was income suppression at the cash counter. The auditor then decided to apply a walk through test of the collection system and bought a lunch cash memo. The cash memo which was issued to him seemed quite normal. He asked one of his team members to try out the same thing on a different day. Again, the cash memo seemed normal. However he saw that the cash memo serial number (a six digit number) was the *same as his own cash memo* of the earlier day, though the date was different. This was strange and he felt that something was wrong with the cash memo. He discussed the matter with the vendor who had supplied the software and explained to him this strange anomaly. The vendor took one look at the cash memo and straight away stated that the cash memos which the auditor had, *were not generated by his software*. The serial number could not be repeated in the same month as a measure of internal control in the software itself. The auditor then asked him how could these cash memos be generated? Simple, by using sophisticated software, almost any kind of bill invoice, memo, form could be replicated as many times as was needed, the vendor informed him. Now the auditor began to see light. On launching a full scale investigation, it was revealed that the cashier would have both the softwares loaded on his terminal, and when he saw an opportunity, particularly of single customers walking in, he would exit from the official cash collection software, and run the other software which had a replicated version of the cash memo with the current date, and print it out. The customer would pay him and take the memo to get a table allotted. *The money against this cash memo would be pocketed by the cashier, since the official cash memo system would not have this transaction at all*. The cashier was smart enough to change dates to be on-line with the current date, but he could not change the numbers. His risk of getting caught was minimal because all such fraudulent cash memos were issued to different customers and no one would be expected to compare numbers. Moreover he would perpetrate this fraud generally for single customers who would not attract too much attention and have minimum of disputes regarding any cash memo. This fraud went un-noticed for almost 3 years and the damage exceeded Rs.20 lacs and the cashier in this manner pocketed a large sum. This fraud was revealed so simply by this digital analysis. Consider the flip side of *not* using this audit approach. While the fraud may have been detected using other audit procedures also, chances were slim.

This illustration does not in any way reduce the importance and effectiveness of traditional audit procedures. However it accentuates the need to treat audit *as a science as well as an art*. Nothing should be treated as standard and routine. The very essence of a professional service is to provide meaningful results. This is possible only when constant refinement, improvement and betterment of services are sought. Revolutionary changes must be brought where useful to supplement and enhance results produced by the time-tested old procedures and techniques.

Chapter 4: Elements of Interviewing

Interviewing is an art which generally is innate or cultivated with experience only. It is important perhaps in every sphere of activity but is indispensable in audit, forensic activities and investigations. In most curriculum of professional examinations, this aspect is virtually omitted or lightly touched. However to get to the bottom of any inquiry an opportunity must be given to all witnesses and suspects to convey and explain the subject matter being inquired into.

During the session on interviewing several excerpts from real interviews will be shown. These indicate the behavioral aspects as well as state of mind of the interview. The state of mind could range from extreme fear to arrogance or from friendliness to sullenness. A good forensic accountant must:

a) Learn to judge the true character of a potential suspect and also of a witness to appreciate or discount the testimony and information given.
b) Cultivate the art, which is possible only with experience, of spotting a liar.

Let us first consider what goes into judging the true character of a suspect. The following two golden rules are very useful and are used by police, enforcement officers and others in criminal investigations

Rule 1. The true character of an individual can be best judged from his behavior when he is alone or outside away from his usual family and office colleagues. When an individual is alone or away from his usual circle of colleagues, and is confident that no one known to him is watching, his behavior is unrestricted and the true traits of that person are evident. For example a very strict obedient person will even spit on the road if he thinks no one is watching. Similarly, it may be found that an otherwise calm and meek person is actually quite an aggressive and unruly person. Or, a person who is soft spoken and sweet tongued, uses brash and abusive language. A disciplined person may not really be so disciplined when he is in a different territory. For an official interview this is not possible or easy to observe, but it is worthwhile to interview suspects and witnesses outside the office using field visits and pretext calls.

Rule 2. The character of a person, particularly a male suspect is also evident from the way the person looks at the opposite sex. Veering lustful looks indicate weak and indiscipline character and susceptibility to do wrongful acts.

Apart from the above two rules, one important and useful trait that an interviewer can be mindful of is whether the suspect is a genuine sportsman or a talented artist. It is a general rule that music and sport lend refinement to character so the chances of sportsmen or artists being severely dishonest are fewer.

<u>The next matters is: How to spot a liar?</u>

The techniques below may show you how to tell if you are being lied to. These techniques are used by government agencies for interrogation. They can easily be utilized in relationships and in business situations. To make successful use of these indicators, it helps to know the suspect's ‘normal' body language and reactions to different situations.

1. **Movements -** Expressions will be stiff. Liars will use fewer hand movements and take up less space. All physical actions will generally take up less space than usual.
2. **Face touch -** Liars will touch the area around their lower face, i.e. scratching the nose, touching the lips or chin. This is an instinct from birth, much like when a child covers his own mouth after a lie, only it has developed through age into less obvious actions.
3. **Eye movement** - The eyes of dishonest people will tend to move around a lot to avoid meeting your gaze. However, staring at your eyes for prolonged periods is also an indicator of a lie. This is often because liars have learned that their eye movements are a giveaway and they are trying to control them.
4. **Pupils** - Pupils will dilate when a lie is told; this is due to the adrenalin being pumped into the body. This factor will also depend on the severity of the lie. Small white lies may not dilate the pupils.
5. **Stance** - Liars often feel uncomfortable standing directly in front of an accuser and may avoid standing with their shoulders squared to yours. Instead, they might stand slightly to the side or with their shoulders offset.
6. **Expressions -** Expressions are limited to the mouth, e.g. if a liar fakes a smile, he will only use selected muscles whereas a natural smile utilizes muscles over the whole face.

7. **Palms -** Liars often try to hide the palms of their hands. This is also instinctive. Hands behind the back or in the pockets are also positive indicators.
8. **Objects -** Liars will play with objects in their possession such as a handbag, bracelet, mobile phone or hair. They may also put an obstruction between themselves and the other person, often something as simple as a coffee cup. This is a subconscious way of attempting to ‘barricade' themselves to relieve the tension of lying.
9. **Tone -** A liar's tone of voice is often not consistent with his/her gestures or statements.
10. **Sarcasm -** Dishonest people will often use sarcasm when answering accusations.
11. **Answers to questions -** A liar uses your words to answer questions, e.g. Q: "Did you have sexual relations with this woman?" A: "I did not have sexual relations with that woman."
12. **Too many details -** Dishonest people will add unnecessary detail to the conversation; this is an attempt to comfort the other person.
13. **Nonsensical -** Often liars' words won't make sense and their grammar may be incorrect. This is because a liar's mind is racing in search of a convincing answer and the signals to the mouth are sent incorrectly.
14. **Avoiding direct answers -** Liars sometimes imply answers instead of denying something directly. This allows them to avoid lying by not making admissive statements. By doing this, it gives them the possibility of going back on their answers and changing them.
15. **Defensive -** Guilty people usually get defensive at the first indication of an accusation whereas honest people will get offensive.
16. **Subject -** A liar will often change the subject; a liar will be comfortable with the change with the belief that his lies have been believed. If honest, a person would be confused as to why a potentially serious subject would be changed. He would be more likely to disregard the subject change and pursue the original conversation.

It's important to note that these indicators experienced individually may not indicate a lie. You will need to look for several consistent indicators, or a combination in a short space of time. Lastly, you may want to take a look at one of the higher quality dating blogs for more advice.

Chapter 5: **Field investigations and use of tools and electronic devices within legal rights**

Field investigations are carried out to make an investigation comprehensive and three dimensional. Regular audits and reviews are merely two dimensional in that they refer to records and books of account. However as they say the proof of a pudding is in its eating. So also the proof of incomes, expenses and assets is in their existence and genuineness. Field inquiries cover the following (an inclusive list, not and exhaustive list):

- Physical verification of assets like stocks, inventories, cash and fixed assets to ensure that they are in existence and in harmony and agreement with the state of affairs indicated in the books of account and relevant records
- Physical presence during payment of expenses such as wages or labour payments. This step attempts to ensure that there are no phantom workers and that unpaid wages are treated and accounted for correctly.
- Verification of proof of investments to satisfy the stakeholders that the investments are in existence and genuine
- Inquiries with third parties as regards the correctness of receivables and payables to ensure that neither are inflated or deflated for malicious purposes
- Visit to scrap yard to determine scrap records, income generated and to ensure that there is no siphoning off of funds
- Visit to ex-employees to gain valuable information during investigations about their awareness of wrongdoings. They may provide useful information which they may have been scared to do during their employment
- Presence during receipt of important and expensive materials, deliveries and other trading transactions to determine whether there are leakages or abuse in purchase or sales.
- Post the Satyam fraud in 2009, many audit firms have even started sending their representatives to banks to get authentic bank confirmations, statements and information relevant to their inquiries.

The above list of field inquiries is endless. The materiality of subject matter being investigated and the cost benefit ratio of such field inquiries generally determine whether these inquiries are necessary.

Aids to field investigations:

There are various tools available in the market to facilitate field inquiries. Essentially these help in making ‘electronic’ notes or records of such field inquiries. When used with legal advice, the following tools can be very useful:

- Mobile cell phones for taking photographs, voice and video recordings of any of the visits listed out above
- Computer laptops during interviews of witnesses and suspects
- Wide range of electronic gadgets concealed in pens, clocks, wearing apparel to records information as when such field visits are carried out.

However, these should be used after seeking legal advice about the circumstances when such gadgets can be used.

Chapter 6: Computer Aided Audit Techniques and Tools (CAATTs)

Audit in general and fraud investigation in particular is getting complex day by day primarily due to migration to non-paper based systems. Processes and workflows are system driven and generally the entire control revolves around the computerized environment. Therefore, there is a clear trend that auditors would have to churn voluminous digitalized data as auditable records. Needless to say, auditors would therefore have to devise ways and means of verification that is commensurate with the changing times. The challenges are to examine various databases generated from different systems which may or may not be integrated.

Changing patterns of businesses, regulatory framework, scarcity of resources at auditors' disposal on one side and the ever increasing mountainous data on other hand is making audit a complex process. Use of CAATTs is, thus, indispensable to the Auditors and forensic accountants.

Let's see how we can use CAATTs in its simplest form for routine work.

Computer Aided Audit Tools or CAATs can be broadly divided into

- Generalized Audit Softwares (GAS) or
- Common Software Tools (CST)

Generalized Audit Software (GAS)

These are specialized softwares designed for accountants fostered with audit architecture in mind. The user interface is very simple for users to follow and with that objective, GASs very often have out-of-box-integration with leading accounting / other systems. However simple it may sound, it needs some training and experience to use them and some people do find it complex to operate. Another reason for GAS's unpopularity is due to its high cost. Some examples of GASs are ACL, Idea, etc.

Pros and Cons of Use of GAS:

- Easy GUI: since these packages are essentially designed for auditors the Graphical User Interface (GUI) provides an easy-to-use mechanism for any standard audit functions.

- In-built audit commands: at just click of few buttons, assorted analytical reports are instantly available. Most of these reports also do provide drill down facility and hence anomalies can be easily identified.
- Logs and Working papers: In current times, many auditors have been facing legal actions by way of class-action suits, etc. for deficiencies in services. GAS tools create logs of all the processes applied and thus can be part of the audit working papers and produced before Court whenever challenged.
- Besides the above, logs also provide an effortless re- processing of similar procedures in future e.g. for repeated quarterly audits.
- Competitive priced: As compared to the other reports generated using software codes, GAS tools are reasonably priced and available on SAS basis also.
- Following could be possible disadvantages. These tools are available on Auditor's machines and clients at times do not allow their confidential data to be copied outside their servers. In that case, there could be tricky situation where the GAS software cannot be copied on Clients server (for license conflicts) and data cannot be copied on Audit servers (to protect confidentiality) and therefore GAS tools cannot be applied. Also, GAS tools need some orientation and training and knowledge of database is essential before GAS can be meaningfully applied.

Common Software Tools (CST)

Due to shortcomings of GASs, CSTs have become popular over a period. Spreadsheets (like MS Excel, Lotus, etc.), RDBMS (like MS Access, etc.) and Report writers (like Crystal reports, etc.) are few examples of CSTs. Their widespread acceptability is due to its instant availability and lower costs. While spreadsheets may be extremely easy to use due to its simplicity and versatility, other CSTs may need some practice.

Whether one uses GAS or CST, it is imperative that the auditor is aware about the manner and processes that have led to the data generation, the control environment revolving around the data and the source from where the data samples are imported into the GAS/CST.

Factors to be considered by the auditor while planning an audit using CAATTs

- Audit objective should be clearly defined.
- Knowledge of database in general and specific familiarity with the auditable data with comprehensive information about data structure and its contents.
- IT knowledge, experience and proficiency of the audit team particularly the current and future users of audit team.
- Availability of the CAAT-Tools vis-à-vis its cost and adaptability to the computer framework of the audit environment.
- Impracticability of manual tests
- Achievability of overall effectiveness of manual test vis-à-vis data mining outputs
- Time and Cost constraints

As a part of computer-aided audit, an auditor needs to do one or more of the following.

A typical 8-point CAATT program :

1. **Check Missings**
2. **Check Duplicates**
3. **Round Numbers**
4. **Repetitive Odd-Numbers**
5. **Classification**
6. **Stratification**
7. **Single Transactions**
8. **Isolated Outliers**

1. Check Missing :

Here we basically try to identify the gaps in any workflow that has serial control mechanism. For example, missing cheques numbers, insurance policies numbers, bank fixed deposit receipts, good received notes, cash receipt numbers, etc. Depending upon the availability of data vis-a-vis audit objectives, an appropriate data-attribute (data field) may be selected to run this check. Missing gaps can be filtered for auditee's explanations.

In one of the Company there were a few missing cheque numbers that could not be physically traced. Nor were proper explanations available whether they were factually cancelled or missing. Later it was revealed that the accountant had pilfered them and in fact one of the adjacent cheque number was surreptitiously encashed too. In another case, a missing Bank Guarantee document was misused to help an accomplice qualify for eligibility criteria in a Government Tender.

2. Check Duplicates :

This is converse of 'Check-Missings'--- the serial control numbers which ought not to be repeated are checked for duplicates. Thus all the documents (that have serial control), mentioned in the above paragraph can be checked for replication. Duplicated numbers could throw up serious gaps in the sourcing of these documents or in case they have been generated using some computerized system could mean a software bug. All such duplicated numbers need thorough detailed review to dispel any wrong doing.

Here auditor can also check duplication of clustered-fields. That is, say a cluster of vendor_code + bill_number can be checked for duplication, presence of which could indicate excess/double payments to same vendor. This is sometimes referred to as 'Same-Same-Different' check.

► Example

An internal auditor was once conducting a risk profiling of a Company in its Head-office by reviewing vendor management of another city branch. He examined the vendor master database by running a duplication check on the telephone number field. Before doing that, he obtained employee master and combined it with the vendor master.

Please refer to the Appendix to this chapter to see how a duplicate check can be performed using MS Excel. The check threw up various duplicated records and the following details were interesting to be noted.

RecNo	Code	Name	Tel1	Tel2	Tel3	Tel4
09635	VA078	A****** Traders	02#-2493##23			02#-6532##54
23852	EG032	G****** S*********	02#-6532##54			

The codes of vendors begins with 'V' and employees codes begins with 'E'. The telephone no. 02#-6532##54 (highlighted above) of A-Traders matched with employee GS. Now that was strange. Readers are again advised at this stage to ponder for a moment of what next steps they would apply to logically go after the foregoing red flag. Make a list of your audit plan before reading further.

General standard process would guide one to verify the purchase orders, bills and payments of A-Traders. Some would also take extreme steps to call for interview of A-Traders and/or GS and question them. Some may want to call up the number to check or cold call for a product or service or visit the address to check ground realities. All these are no doubt good steps, but the point to be noted is that these may send an alert and many times an evidence is lost if the perpetrators are forewarned by such alarms.

In line with a thinking different attitude, the Auditor is this case called for all emails received or sent to A-Traders (say atraders***@gmail.com) from the company's email server database. This resulted in some ~500 emails exchanged at various times. A little scrutiny of these when compared to email boxes of GS and his assistant TR, revealed that few emails pertaining to a subject 'roof leakage in kitchen area' were missing from personal email boxes of GS and TR. These were strange, since traces of emails with aforesaid subject could be seen with 'cc' marked to Company's Vice-President and COO. Further investigation revealed the following modus operandi of the fraud. GS and his assistant, TR created a business name A-Traders and employed a technician who would carry out the civil jobs. They made him proprietor but kept control over the banking and office set-up. GS had many houses some of which were let-out on rent and one of his earlier small house was given business address of A-Traders. The old telephone no. was used as fax and since the organization had all forgotten residential telephone numbers (as in last year's mobiles phones were used more often), this was deemed unsuspecting. Thus GS, sitting in his office could virtually managed the business of A-Traders. Most of the email communication was sent from official email to the gmail_id and vice versa using his handheld smart phone. Once GS had to inspect one the Company's client and there were some heated arguments with a customer about the leaking roof. In the fit of the rage, GS immediately shot out an email to distance Company from the problem by sending some pictures clicked at the site. Not realizing, the email by mistake was sent from the Gmail_id instead of the official id. Later the Customer got into the email-war by marking that email to several people in both the organisations. The email tennis-match went off for some time, when GS discovered the error about the gmail_id being incorrectly used. Since no one had noticed that, he quietly got all those email deleted from TR account and his own email box (there were a few official emails too). The higher-ups (Vice-President and COO) didn't noticed because they never got involved with the subject issue and any organizational heads are spammed with these trivial issues which are best ignored. The Auditor got clue about the collusion and the deletion provided the relevant evidence. GS could not explain how the email to customer got initiated by A-Traders who had no connection whatsoever as also various other content matter which only GS knew about besides the story of email deletions thereafter. GS had no option but to confess and the Company also recovered some of the losses.

This case study explains the need to have a strategy in investigation and more than that a forensic view to think differently. No doubt the conventional plans are important but sometimes a different thinking may give quick and meaningful results. There is nothing like a perfect murder and perpetrator will leave some trace of a footprint since all things may not be in his/her control.

3. Round Numbers :

Basically there is nothing wrong with Round numbers and it is not unusual to see many round number transactions in any commercial deals. However, sometimes round numbers are symptomatic of mysterious deals. Therefore the auditor should use some judgement to eliminate possible round number cases. For example, it is quite natural to generally spot round number transactions in monthly rentals, professional fees, audit remuneration, etc.- these transactions could be filtered out from the list of transactions with round numbers.

Daily Times was a reputed newspaper publishing company that was publishing an eveninger-tabloid. Several round numbers payments were noticed to M/s. ABC Ltd., a news sprint supplier. ABC had been dealing with Daily Times for last 3 years and ever since payments to the vendors was always in round numbers. A detailed review and visit to ABC, revealed that there were several gaps in accounting of both the entities. Just to keep these gaps under the carpet, 'on account' payments in round numbers were affected to the vendor. Daily Times would adjust the bills per its own accounting system and ABC would follow theirs. Investigations exposed large unaccounted transactions of unsold newspapers returned back (for recycling).

4. Repetitive Odd-Numbers

This is converse of Round-numbers. Unlike the round numbers, repetition of odd numbers (particularly repetitions at decimals levels) are very rare coincident. Unless of course there is apparent reasons say, like for telco having promotional offer of Rs 199/- pre-paid packs – but in that case, the repetitions will be by volumes and not a few stray incidences here and there. Repeated odd-number transactions can be filtered for detailed verification and most often these will throw up some irregularities.

In one MIS report of a public company running a restaurant business, the tobacco sale of Rs. 10,89,233/- was repeated consequently for the month of June and July. This was too much of coincident to catch the attention of the independent director who was otherwise a reputed investigator in his professional life. A few probing questions during the audit committee meeting revealed that the Manager was faking the MIS numbers and the amount was result of sloppy use of the spreadsheet's copy-paste command. The Manager had been manipulating MIS reports for quite some time and over the period casual complacent attitude had set-in. A detailed investigation launched subsequently exposed other mismanagement.

Repetitive checks can be performed on a given sub-set or across the entire set of population. For example, say in case of database of purchase records -- this check can be applied separately for each vendor or across all the vendors.

5. Classification

Classification is a process of arranging data into homogenous group or classes according to some common characteristics present in the data. This analysis aid the Auditor in getting a bird's eye view to see a panoramic whole of how the data is dispersed or where the concentration lies. Classification can be combined with other appropriate CAATT checks to enable more penetrative tests.

Classification could be done on various attributes (field) of data. For example, classify the data vendor-wise, salesman/agent wise, account wise, period wise, day-timing wise, etc. A typical classification of Purchase Data can be done to get following result

Sr	Party_Code	Count	Sum_Amount	%Count	%Amt
1	A-0001	3	7,375	0.09%	0.06%
2	A-0002	4	3,548	0.12%	0.03%
3	A-0003	107	46,430	3.26%	0.40%
4	A-0004	68	8,756	2.07%	0.07%
5	A-0005	1	188	0.03%	0.00%
321	Y-0006	1	17,329	0.03%	0.15%
322	Y-0007	1	2,696	0.03%	0.02%
323	Y-0008	1	447	0.03%	0.00%
324	Y-0009	3	26,989	0.09%	0.23%
325	Z-0001	21	5,940	0.64%	0.05%
326	Z-0002	13	9,496	0.40%	0.08%
327	Z-0003	2	165	0.06%	0.00%
328	Z-0004	1	56	0.03%	0.00%
Total Vendors =328		**3283**	**1,16,83,516**	**100.00%**	**100.00%**

The above list running into several pages can be further filtered for say %Count<1% and %Count >0.5% to get a very small sample size as follows :

Sr	Party_Code	Count	Sum_Amount	%Count	%Amt
16	A-0016	20	4,26,636	0.61%	3.65%
23	A-0023	13	15,94,532	0.40%	13.65%
34	A-0034	28	88,301	0.85%	0.76%
73	A-0073	3	99,358	0.09%	0.85%
96	A-0096	7	61,264	0.21%	0.52%
145	D-0002	14	1,66,954	0.43%	1.43%
149	D-0006	7	1,36,835	0.21%	1.17%
155	E-0006	7	2,30,400	0.21%	1.97%
179	I-0001	4	1,47,862	0.12%	1.27%
185	I-0007	10	68,497	0.30%	0.59%
207	L-0001	8	3,41,660	0.24%	2.92%
227	M-0019	4	5,09,856	0.12%	4.36%
238	N-0004	6	67,089	0.18%	0.57%
257	P-0009	1	1,07,361	0.03%	0.92%
260	P-0012	1	59,967	0.03%	0.51%
290	T-0004	12	3,02,458	0.37%	2.59%
301	T-0015	28	4,27,933	0.85%	3.66%
306	U-0003	1	1,52,343	0.03%	1.30%
Total Vendors = 18		**174**	**49,89,306**	**5.30%**	**42.70%**

As can be seen above, the sample size has generated just 18 vendors accounts covering 5% in terms of volume and 42% in terms of value.

In Excel the Pivot-Table procedure can be applied to classify the data instantly in multiple ways.

6. Stratification

Stratification is a derivative of classification which involves grouping of large data into 'strata'. Strata means levels, bands or groups. Thus it involves dividing or rearranging the data within the Strata and then overviewing it to decipher the latent configuration of the database.

For example the purchase data of the above example can be stratified into various bands of bill values to obtain following results :

Strata		Bill Counts			Bill Value		
Bill_Val_From	Bill_Val_To	Count	Count%	Cumm%	Sum_Bill_Val	%	Cumm%
-	10,000	3081	93.85%	100.00%	34,49,671.74	30%	100%
10,001	20,000	77	2.35%	6.15%	11,14,929.05	10%	70%
20,001	30,000	45	1.37%	3.81%	11,35,250.64	10%	61%
30,001	40,000	37	1.13%	2.44%	13,47,267.34	12%	51%
40,001	50,000	13	0.40%	1.31%	6,01,560.32	5%	40%
50,001	1,00,000	14	0.43%	0.91%	9,17,721.94	8%	35%
1,00,001	1,50,000	7	0.21%	0.49%	8,68,979.09	7%	27%
1,50,001	3,00,000	7	0.21%	0.27%	14,40,783.65	12%	19%
3,00,001	4,00,000	1	0.03%	0.06%	3,19,000.00	3%	7%
4,00,001	5,00,000	1	0.03%	0.03%	4,88,352.19	4%	4%
		3283			1,16,83,515.95		

As can be seen, a sample size can be easily determined from above to mark bill values over Rs 50,000/- (depicted by dotted line in table above). This translates into a 0.91% in volume terms and 35% in value terms.

Strata can be quantities, insurance-policy holder-agewise, debtors ageing analysis, etc..

In Excel, apply groupings after classification of data using Pivot Tables. Depending upon data, groupings can be in various forms. For example, for date-time field, grouping options can be on hours, days, quarters, years, etc.

7. Single Transaction

This is self-explanatory and may need little explanation. As the name suggests, this check basically filters all the single transactions in a database. These single records could be bonafide cases or just a stray transaction inserted by opportunist beneficiary. Generally vendor account, employee account, customer account, etc. should have multiple transactions since everyone wants regular business. Solitary transaction could be vouchsafe to exonerate sketchiness if any.

In a database of a medical distribution arm of a pharmaceutical company (Pharmaco), it was noticed that there were many stray records of doctors who were reimbursed train fares as part of promotional scheme. The promotional offer was to incentivize the doctors by allowing them tourism along with their family. The Pharmaco regularly had these schemes -- at lower end it was distribution of some token, gifts, etc. whereas at higher end senior doctors were allowed foreign travels, costly medical equipments, etc. The database analysis of doctor-wise expense of last 3-4years revealed these stray instances. While the individual vouchers did not throw up any irregularities, collectively all these single instances had a pattern of suspicious behavior. These vouchers were otherwise vouchedsafe with proper supportings (original train tickets), manager's approvals, names and particulars of the doctors, etc. However, collectively viewed the skepticism was obvious; train tickets of many beneficiaries pertained to journeys for same day with same coach numbers – this breached the test of impossibility. Field verification exposed fake names and addresses of many of these doctors, however the tickets appeared genuine. On detailed investigation, it was revealed that the accomplice would collect all the tickets from the Railway-ticket-checker by tipping him a good amount. Suitable tickets (family/groups) were later attached as supportings and monies siphoned off on regular basis. The fraud was perpetrated into small amounts on regular basis aggregating to large amount eventually. Clearly there were many single instances of genuine cases also but that actually facilitated in camouflaging the fraud.

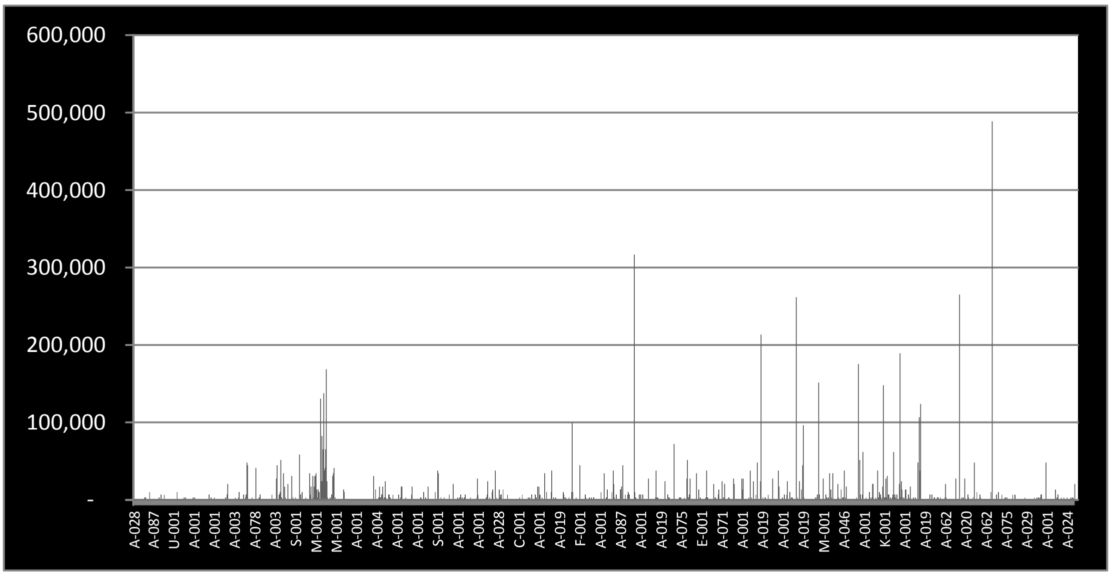
8. Isolated Outliers

An Isolated outlier is an observation in a data set which is far extreme in value from the others in the data set. It is an unusually large or an unusually small value compared to the others. Any database will be vitiated by incongruent records or contaminated transactions which will stick out as outliers. That happens because of its inherent nature that impedes its blending with the others in the group and will be clearly isolated with the remainders.

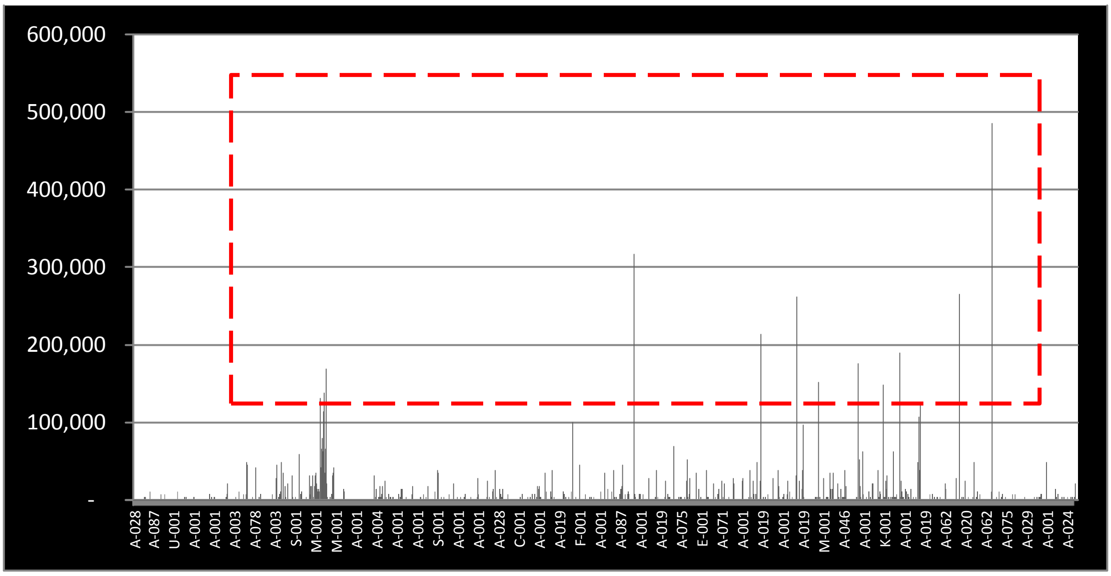
A word of caution -- there could outliers that would creep in any database as deviations which happens in normal course and may not always mean a fraud or an error. However, as an auditor s/he will be concerned about these outliers and should review these transactions as part of audit plan.

There are various ways to spot the Isolated Outliers as discussed below.

- Simple Charting Options : Using a popular spreadsheets, it is not difficult to plot a chart of the entire database as shown below. The database contains 3,283 records of 328 vendors. The vendor codes are plotted against the x-axis and the amount against the y-axis.



A simple visual review of the chart can enable the auditor to immediately spot the isolated outliers. The above chart is reproduced below with the dotted outline :



Thus all the transactions above Rs 1,00,000/- are isolated outliers.

- **Relative Size Factor:**

RSF is the ratio of Largest Number to the Second Largest Number of a relevant set.

$$RSF = \frac{\text{Largest Number}}{\text{Second Largest Number}}$$

For example, if we have following bank payment vouchers of Vendor XYZ

Voucher No.	Rs.
SB-211	50,000
SB-642	5,00,000
SB-547	5,00,000
SB-1864	20,000
SB-4755	23,000
SB-8347	8,500

The Largest value in above table = Rs 5,00,000/- and the second largest value = Rs 50,000/-. Therefore the RSF in this case = 10 that is Rs 5,00,000 Lacs divided by Rs. 50,000/-

Per RSF theory generally any transactions where RSF > 10 are the cases of isolated outliers.

Please refer to chapter 3 for detail discussion on RSF

- **Benford's Law**

This is revolutionary theorem propounded by Dr. Frank Benford, as American Electrical Engineer and Physicists. Benford's Law is also popularly known as the first digit law. The law is about statistical statement regarding occurrence of numerical digits. Dr. Benford observed that in any large database generated through an ordinary process, the natural numbers (numbers which are not limited by boundaries or non-serial nos.) follow a count of its first-left-most digit which is not in consonance with the law of probability. He asserted that the first-leftmost-digit (e.g. it is "1" in a number 1,23,456.78") follows a pattern of appearance where the lower numbers have more chance of appearing as compared to the higher numbers. According to him the appearance of first left most digit has the following frequency.

Digit	1	2	3	4	5	6	7	8	9
	30.1 %	17.6 %	12.5 %	9.7%	7.9%	6.7%	5.8%	5.1%	4.6%

Thus numbers deviating from the above principle would be transactions that could are isolated outliers.

Please refer to chapter 3 for detail discussion on Benford's Law.

Notes