P 948 Jyoti Kumari(Research Fellow)

Very Good morning to all of you, I think it is time to begin, because others are still doing breakfast and don't know what time they will come,6 are over here and 6 are doing their breakfast, so let them do their breakfast, and we begin our session nonetheless. The timing was told to them i.e nine o'clock. so, may be we can start with brief introduction. Can all of you tell about yourself.....I am.....no no please keep sitting no body need to stand, I am from Himachal Pradesh...2014....Allahabad.....We have Hon'ble Judge Santosh Hegde,very renowned Judge, we were in awe of him, then we have Hon;ble P P Naolekar Lokayukta from Madheya Pradesh, then we also have Mr. Rakesh Jain Deputy CAG who will be taking us to procurement fraud. I will take one minute in explaining why this course and what are the objectives of this course. As a High court Judge u r in some committee or the other, if I am not mistaken. You wd be buying some very small thing like stationary or big thing like computers, video conferencing equipments, otherwise also we upgrade ourselves as an institution. After a gap of five years things are to be bought/upgraded/changed, so one way or the other we all are involved in some kind of economic activity.evee though we are in some kind of service. it no more effects private industry only,it effects every industry, every institution and every organization, for example you will issue tender

I will tell you my experience, there is a CVC guideline, you sd ask for turnover of 30% of value of your project, sometime we don't know because we are of different background. draft of tenders are done and things are brought in our notice and then tenders are floated and we see that no body is turning up. and this keeps on happening for three four years. then some one comes and tells us that your norms are above the prescribed limit set by CVC. Small small things we dont know and we suffer. So this is a program where we learn preventive and other strategies to overcome economic crime in our own sector. There are other small small things related to procurement. we have purchase committee, anything which is below one lakh need not go for tender. Again u will see that there are big loopholes in that sector also. Suppose u r not a local of that area there are many opportunities to make a fool out of you. Because you really dont know the length and breadth of that Jurisdiction. and who is buying what n where and under what pretext. These are all small things that u learn from your administrative experience during the years. So economic crimes are something which is not related to the particular industry but to everyone of us. That's why this conference is all about identifying the economic crime that we generally overlook because we have other duties and which are the sectors affected by the economic crime. One of the sessions is State and Govt owned enterprises to be taken up by Justice U U Lalit. this is the program to tell us what are the crimes of economic nature that actually effect us without our knowing us that we are being affected and unknowingly are being victim of these economic crimes. With this brief

introduction now I leave you all to Hon'ble Justice P P Naolekar to take his session on asset misappropriation.

Good morning to all of you. Today we are talking about economic crime. Economic crime are fraud,cyber crime, asset misappropriation and accounting fraud. Corruption erodes integrity and disrupts the life. Corruption in the Indian society has prevailed from time immemorial in one form or the other. The basic inception of corruption started with our opportunistic leaders who have already done greater damage to our nation. People who work on right principles are unrecognized and considered to be foolish in the modern society. Corruption in India is a result of the connection between bureaucrats, politicians and criminals. Earlier, bribes were paid for getting wrong things done, but now bribe is paid for getting right things done at right time. Further, corruption has become something respectable in India, because respectable people are involved in it. Social corruption like less weighing of products, adulteration in edible items, and bribery of various kind have incessantly prevailed in the society.

In today's scenario, if a person wants a government job he has to pay lakhs of rupees to the higher officials irrespective of satisfying all the eligibility criteria. In every office one has either to give money to the employee concerned or arrange for some sources to get work done. There is adulteration and duplicate weighing of products in food and civil supplies department by unscrupulous workers who cheat the consumers by playing with the health and lives of the people. In the assessment of property tax the officers charge money even if the house is built properly according to the Government rules and regulations.

Political corruption is worst in India. The major cause of concern is that corruption is weakening the political body and damaging the supreme importance of the law governing the society. Nowadays politics is only for criminals and criminals are meant to be in politics. Elections in many parts of the country have become associated with a host of criminal activities. Threatening voters to vote for a particular candidate or physically prevent voters from going in to the polling booth – especially weaker sections of the society like tribals, dalits and rural woman occurs frequently in several parts of the country. Recently, the Government increased the salary of the M.P.'s from Rs.16, 000 to Rs.50, 000, that is 300% increase to the existing salary. But many of them are unhappy with rise and want the Government to increase the salary to a much more extent. This clearly shows how the politicians are in constant thirst for monetary benefits and not caring about the welfare of the people. Tax evasion is one of the most popular forms of corruption. It is mostly practiced by Government officials and politicians who lead to the accumulation of black money which in turn spoils the moral of the people.

1. The most important factor is the nature of the human being. People in general, have a great thirst for luxuries and comforts and as a result of which they get themselves involved in all unscrupulous activities that result in monetary or material benefits.

2. Moral and spiritual values are not given utmost importance in educational system, which is highly responsible for the deterioration of the society.
3. The salary paid to employees is very less and as a result of which they are forced to earn money by illegal ways.
4. The punishments imposed on the criminals are inadequate.
    1. The political leaders have spoiled the society completely. They lead a luxurious life and do not even care about the society.
    2. People of India are not awakened and enlightened. They fear to raise their voice against anti-social elements prevailing in the society.

1. The Right to Information Act (RTI) gives one all the required information about the Government, such as what the Government is doing with our tax payments. Under this act, one has the right to ask the Government on any problem which one faces. There is a Public Information Officer (PIO) appointed in every Government department, who is responsible for collecting information wanted by the citizens and providing them with the relevant information on payment of a nominal fee to the PIO. If the PIO refuses to accept the application or if the applicant does not receive the required information on time then the applicant can make a complaint to the respective information commission, which has the power to impose a penalty up to Rs.25, 000 on the errant PIO.
2. Another potent check on corruption is Central Vigilance Commission (CVC). It was setup by the Government to advise and guide Central Government agencies in the areas of vigilance. If there are any cases of corruption or any complaints thereof, then that can be reported to the CVC. CVC also shoulders the responsibility of creating more awareness among people regarding the consequences of giving and taking of bribes and corruption.
3. Establishment of special courts for speedy justice can be a huge positive aspect. Much time should not elapse between the registration of a case and the delivery of judgment.
4. Strong and stringent laws need to be enacted which gives no room for the guilty to escape.
5. In many cases, the employees opt for corrupt means out of compulsion and not by choice. Some people are of the opinion that the wages paid are insufficient to feed their families. If they are paid better, they would not be forced to accept bribe.

The one thing that needs to be ensured is proper where the good, patriotic, intellectuals come forward to serve the country with pride, virtue, and honesty for the welfare of the people of India., impartial, and unbiased use of various anti-social regulations to take strong, deterrent, and timely legal action against the offenders, irrespective of their political influences or money power. Firm and strong steps are needed to curb the menace and an atmosphere has to created to curb corruption. Lokayukta Act Received the assent of the President on the 16th September, 1981. Assent first published in the " Madhya Pradesh Gazette (Extra- ordinary)" dated the 15th October, 1981). An Act to make provision for the appointment and functions of certain authorities for the enquiry into the allegation against "Public Servants."1 and for

matters connected there with. Be it enacted by Madhya Pradesh Legislature in the Thirty – second year of the Republic of India as follows: - 1. Short title, extent and commencement: – (1) This Act may be called the Madhya Pradesh Lokayukt Evam Up-Lokayukt Adhiniyam, 1981.
(1) It extends to the whole of the State of Madhya Pradesh.
(2) It shall come into force on such date2 as the State Government may, by notification, appoint.
2. Definitions: –
In this Act, unless the context otherwise requires –
(a) "officer" means a person appointed to a public service or post in connection with the affairs of the State of Madhya Pradesh;
(b) "allegation" in relation to a public servant means any affirmation that such public servant,
(i) has abused his position as such to obtain any gain or favour to himself or
to any other person or to cause undue harm to any person;
(ii) was actuated in the discharge of his functions as such public servant by
improper or corrupt motives:
(iii) is guilty of corruption; or
(iv) is in possession of pecuniary resources or property disproportionate to his
known source of income and such pecuniary resources or property is held
by the public servant personally or by any member of his family or by some other person on his behalf.
Explanation:–
For the purpose of this sub-clause " family" means husband, wife, sons and unmarried daughters living jointly with him;
(c) " Up-Lokayukt " means a person appointed as a Up-Lokayukt under
Section - 3;
(d) "action" means action by way of prosecution or otherwise taken on the report of the Lokayukt or the Up-Lokayukt and includes failure to act, and
all other expressions connecting action shall be construed accordingly;
1 The words " public servants" substituted for the words "certain high dignitaries and others vide the
Madhya Pradesh Lokayukt Evam Up-Lokayukt (Sanshodhan) Adhiniyam, 1986. Published in M.P.
Rajpatra dt. 9 Jan.1987 (p.91) 2 This Act shall come into force from 14 th Feb. 1982, vide Notification No. F-E5 (6) – 198 –1-5 dt. 14 th Feb. 1982, published in M.P. Rajpatra (Asadharan) dt. 14-2-82, p. 161.
(e) "Minister" means a member of the Council of Ministers by whatever name called for the State of Madhya Pradesh, that is to say.(Chief Minister)1, Deputy Chief Minister, Minister, Minister of State, Deputy Minister and Parliamentary Secretary
(....) 2,3and shall include Neta Pratipaksha as defined in clause A of section 2 of the Madhya Pradesh Vidhan Mandal Neta Pratipaksha (Vetan Tatha Bhatta) Adhiniyam, 1980 (No. 8 of 1980)" (f) "Lokayukt" means a person appointed as the Lokayukt under section 3;

(g) “Public servant” means a person falli
ng under any of the following categories,
namely :-
(i) Minister;
(ii) a person having the rank of
a Minister but shall not include Speaker and
Deputy Speaker of the Madhya Pradesh Vidhan Sabha;
(iii) an officer referred to in clause (a);
(iv) 4[an officer of an Apex So
ciety or Central Society within the meaning of
clause (t-1) read with clause
s (a-1) , (c-1) and (z) of section 2 of the Madhya
Pradesh Co-operative Societies Act, 1960 (No. 17 of 1961).”
(v)5[Any person holding any office in , or any employee of –
(i) a Government Company within the meaning of section 617 of the
Companies Act, 1956; or
(ii) a Corporation or Local Authority established by State Government
under a Central or State enactment.
(vi) 6(a) Up-Kulpati, Adhyacharya and Kul Sachiva of the Indira Kala Sangit
Vishwavidyalaya constituted under section 3 of the Indira Kala Sangit
Vishwavidyalaya Act, 1956 (No. 19 of 1956);
(b) Kulpati and Registrar of the Jawaharlal Nehru Krishi Vishwavidyalaya
constituted under section 3 of the Jawaharlal Nehru Krishi Vishwavidyalaya
Act, 1963 (No. 12 of 1963); 1 Word “Chief Minister” inserted by M.P.Amendment Act No.7 of 1982, published in M.P.Rajpatra (Asadhran) dt. 27.3.82 pp. 426-428

So we disperse for the tea break and introspection together and return for the tea. Can we have a big round of applause for Honb'le Justise P P Naolekar.

A very good morning to all of you. I will keep my talk brief to the presentation and then we can have a discission.

Type of Crime : Procurement Fraud

By

Rakesh Jain

Deputy Comptroller & Auditor General

Outline of Presentation

- ❑ Procurement
- ❑ Fraud
- ❑ Existing Instructions
- ❑ Principles laid down by Supreme Court
- ❑ Weaknesses
- ❑ Way forward
- ❑ Salient features of Public Procurement Bill
- ❑ Important Audit Findings
- ❑ Best Practises

PROCUREMENT

United Nations Commission On International Trade Law (UNCITRAL)

Procurement means the acquisition of goods, construction or services by a procuring authority.

United Nations

Procurement functions include all actions necessary for the acquisition, by purchase or lease, of property, including products and real property, and of services, including works.

Public Procurement Bill 2012

‘’Procurement’’ or ‘’public procurement’’ means acquisition by purchase, lease, licence or otherwise of goods, works or services or any combination thereof, including award of Public Private Partnership projects, by a procuring entity, whether directly or through an agency with which a contract for procurement services is entered into, but does not include any acquisition of goods, works or services without consideration, and the term ‘’procure’’ or ‘’procured’’ shall be construed accordingly.

Fraud

Black’s law Dictionary

Fraud consists of some deceitful practice or wilful device, resort to with intent to deprive another of

his right or some manner to do him an injury.

United Nations

Fraud in an act or omission that intentionally misleads or attempts to mislead ,a party to obtain a financial or other benefit or to avoid an obligation.

Government Accountability Office (GAO)

Fraud as a type of illegal act involving the obtaining of something of value through wilful misrepresentation. Whether an act is, in fact, fraud is a determination to be made through the judicial or other adjudicative system.

Procurement Fraud

- Forging documents, preparing false entries in enterprise systems or making false statements to obtain a financial or other benefit to which a person is not entitled.
- Approving/Inflating contracts prices & invoices that are above contractual /market prices.
- Biased supply market research, development of specification favouring a particular product or supplier, favours at the time of bid preparation, receiving of bids , evaluation phase and contract management plan.
- In cost plus contracts, cost/labour mischarging, defective pricing, defective parts, unauthorised product substitution.
- Misuse or theft of a password for the unauthorised access to IT systems.

Executive Instructions

Rules, Guidelines Governing Public Procurement

General Financial Rules (GFR), 2005

- State GFRs
- Delegation of Financial Powers Rules (DFPR), 1978
- Guidelines issued by the Central Vigilance Commission (CVC)
- Guidelines issued by the Directorate General of Supplies and Disposal (DGS&D)

- Manuals on the procurement of goods, services and works issued by the Department of Expenditure, Ministry of Finance.
- Guidelines on procurement issued by individual Ministries / Departments, PSUs etc.
- Legislation on procurement enacted by individual states - Tamil Nadu and Karnataka

Fundamental principles

- Open tendering
- Effective Advertisement
- Non-discriminatory tender conditions & Technical specifications
- Public tender opening
- Award to most advantageous bidder

Principles laid down by Supreme Court

- Government organizations are not allowed to work in secrecy in dealing with contracts, barring rare exceptions.
- Reasons for administrative decisions must be recorded, based on facts or opinions of knowledgeable persons again based on facts.
- Tendering Process or Public Auction is the basic requirement for the award of any contract.
- Adequate publicity is essential.
- Officers engaged in public procurement have to perform fiduciary duty.
- There has to be fair play in the actions for procurement.
- Bid evaluation has to be strictly in accordance with the bid evaluation criteria stated while inviting the bid.

Weaknesses in the existing system

- Absence of a dedicated Policy making Department
- Absence of Legal Framework
- Absence of Standard Documents
- Nomination basis
- Limited number of Suppliers / List of Registered Vendors
- Two Envelope System
- Delay in Tender Processing and Award Decision

- Works contract
- Negotiation

Way Forward

- Public Procurement Law
- Institutional framework preferably dedicated department/unit within the Ministry of Finance
- Standardization including the procedures, tender documents and general conditions of contract
- Competitive bidding should be the norm for procurement unless permitted and justified in special cases
    I. Evaluation criteria should be clearly spelt out in tender documents
    II. Evaluation as per the declared criteria
    III. Public opening of tendering should be mandatory
    IV. Introduce debriefing procedure
    V. Result of the tendering process in the Public domain
- Switch over to e-procurement regime (Korea Online E-procurement System)
- Reforms in works Procurement
    - For all development projects, the executing agencies shall carry out procurement planning (statutory clearances, land acquisition & availability), logistics, contract packaging, scheduling and firming up of funds before sanction.
    - Schedule of rates should be reviewed and revised
    - Contractors past performance data should be maintained
    - Bid capacity – Finance, equipment, personnel & past performance should be mandatory criteria
- Regular Training Programmes
- Performance Indicators

The Public Procurement Bill -Objectives

- A legislation to regulate public procurement by all Ministries and Departments of the Central Government, Central Public Sector Enterprises, Autonomous and Statutory bodies controlled by the Central Government and other procuring entities;
- Ensuring transparency, fair and equitable treatment of bidders, promoting competition and enhancing efficiency and economy in the procurement process;
- Maintaining Integrity and public confidence in public procurement process

Basic Features

- Five Chapters(Preliminary ,Principles & Methods of Procurement ,Institutional Mechanism, Offences penalty& debarement ,Miscellaneous)
- To be supplemented by Rules for procurement of Goods, Works and Services. Separate sets of Rules for:
  - Procurement for the purpose of national security
  - Entering into Public Private Partnerships
  - Procurement by Central Public Sector Enterprises
- Exemptions from the law in certain circumstances
- Key transparency and accountability norms incorporated from international best practices
- Expeditious and streamlines grievance redressal procedure

Fraud Triangle-Dr. Donald R .Cressey

- Motive or pressure – the need for committing Fraud
- Rationalisation – the mindset of the fraudster that justifies them to commit fraud
- Opportunity – the situation that enables fraud to occur

Opportunity Pressure

Rationalization

Key to fraud deterrence is literally breaking this triangle by eliminating one of the three factors

Fodder Scam – Purchase of feed & fodder

- As per approved scale, Rs.10.5 crore were required for feed/fodder for three years. As against this, Rs.279.34 crore were drawn from six treasuries during 1993-1996 for purchase of feed and fodder.
- Yellow maize and groundnut cake constituted 10 per cent and 15 per cent of the composite feed whereas it accounted for 90 per cent of the total purchase. Seven major suppliers accounted for over 80 per cent of the purchases.
- Expenditure on these items during three years were Rs.164.22 crore and Rs.86.54 crore respectively which amounted to excess purchase by 147 times and 55 times of their requirement.

- The Regional Purchase Committee met six months after the issue of tender in October 1992 while the suppliers were given only seven days to respond to the notice inviting tender. Rates decided in 1993 continued till 1996 as the Committee did not meet after 1993.
- Though quality and usefulness of feed and fodder was to be tested by chemical analysis, very few samples were sent to the designated institute in Ranchi for this purpose. Payment for the supplies was made without the test reports in violation of departmental guidelines.
- Vehicles types mentioned in the transport bills for Rs.1.24 crore for transportation of feed and fodder to remote blocks included mopeds, scooters, motorcycle, trekkers, police van, bus, oil tankers and autorickshaw.
- Serious irregularities were noticed in processing of rates and selection of vendors for medicines by the Central Purchase Committee (CPC). The CPC met six months after the receipt of tenders while only ten days time was given to bidders for response. Rates approved in 1991 continued till 1995. Excessively high rates quoted by local firms were approved by the CPC though reputed firms quoted lower rates. The firm, 'Inter Pharma' was approved though there was a vigilance case against them for serious irregularities on supply of equipment during 1985-88.
- Rs.151.50 crore were paid for purchase of medicines in the six districts in 3 years. The districts hospitals and dispensaries confirmed that negligible amount of medicine was actually supplied to them and that no indents of medicines were asked from them.
- Tonics and food supplements which were normally not supposed to be distributed by hospitals and dispensaries accounted for 17 per cent of the total purchases.

- During 1993-94 to 1995-96, huge quantity of equipment/materials for artificial insemination were purchased for Rs.24.28 crore in six districts while number of artificial insemination came down drastically during these years. Most of the artificial insemination units became defunct due to paucity of funds.
- While only 19 lakh insemination were done in three years whereas lubricant and sheaths for artificial insemination purchased by the department could cater to inseminate 84.80 lakh cattles and 22.80 lakh cattles respectively.

DDOs & Treasuries

- The allotment figures had no relation to budget provisions for Animal Husbandry Department. Many fictitious allotment figures of heavy amounts were quoted by the DDOs in the bills. Every month new allotment figures were routinely quoted in South Bihar districts. The Treasury Officers overlooked the absurdness of such figures of

heavy allotments and helped in perpetration of fraudulent drawal of bills on the basis of fake allotments.

- Vouchers for contingency payments had serious deficiencies. Bills (formats were different) were passed by Treasury Officers for payment without the signature of the DDO, supported by large number of sub-vouchers (not defaced/cancelled).

Finance Department

- Excess expenditure of Animal Husbandry Department increased from 21 per cent of its total budget provisions in 1987-88 to 229 per cent in 1994-95.
- Over 80 per cent of the total drawal of Animal Husbandry Department during 1993-94 to 1995-96 was made from the treasuries in Ranchi, Chaibasa, Dumka, Jamshedpur, Gumla and Patna districts. Rs.473.52 crore was drawn towards purchase of feed/fodder (Rs.279.34 crore), medicine (Rs.151.50 crore), artificial insemination equipments/materials (Rs.24.28 crore) and others (Rs.18.40 crore).
- Finance Department was aware about the excess drawals in the Animal Husbandry Department at various stages, but took no action to investigate the excess drawals.
- During 1993-94, the Finance Department banned payment for three schemes of Animal Husbandry Department. Finance Department issued clarifications to the Doranda and Ranchi Treasury Officers to make payment of bills of all items relating to the animals of Animal Husbandry Department up to 16 per cent of Annual Budget Provision even while the ban imposed by them continued.
- On 18.2.94, the Chief Secretaries observed heavy drawals from the treasuries and instructed the Finance Commissioner to enquire on test basis within two days, two or three major Treasuries to ascertain the cause of heavy drawal. There was no evidence to show that such an inquiry of drawals from Treasuries was made.
- Reserve Bank of India, Nagpur sends monthly statement to Finance Department showing the disbursements through each treasury which were not analysed in Finance Department to ascertain the reasons of heavy cash outgo from certain treasuries.

Commonwealth Games 2010

- Award of contracts on single tender basis / nomination basis / irregular payments.
- Award of contract to ineligible vendors, restrictive prequalification conditions to limit competition, inadequate time for bidding, cancellation and retendering of contracts and inexplicable delays in contract finalisation.
- Works relating to construction of flyovers, stadiums, lane strengthening and widening, upgrading street lights, power plant, sewage plants, parking lots, bidding norms were bypassed.
- Rates of some of the items in L1 bid rates were overwritten.

- ❑ Items were purchased/hired at abnormally high prices.
- ❑ Substandard material, delays, quality compromises.

National Rural Health Mission - UP

- ❑ Civil works were awarded on nomination basis. Preference was given to cooperative societies although the accountability structure was not robust.
- ❑ Funds were released to constructions agencies without obtaining detailed estimates and utilisation certificates.
- ❑ Quality control of NRHM works were not ensured.
- ❑ Weak procurement system of Medical Supplies within SHS.
- ❑ Purchases were not made on competitive basis, higher rates on quotation basis, cross verification of invoices through tax authorities shows that they were fictitious.
- ❑ Registers were not maintained

Best Practices in Power Grid

- ❑ Implementation of Integrity Pact
- ❑ Independent External Monitor
- ❑ Single stage two Envelope Bidding procedure
- ❑ Performance based evaluation of the vendors
- ❑ e-procurement from January 2012
- ❑ e-reverse Auction
- ❑ Conductor Inventory
- ❑ Independent Quality Assurance and Inspection Wing

Supply of Subs-standard material

- ❑ All the ACSR Lapwing conductors supplied were to be replaced including which were already strung.
- ❑ Continue to supply of existing orders under following conditions:
  - Correct deficiency in plants
  - Strengthen in-process checks, routine tests etc.
  - Surprise verification of product quality by Power Grid staff
  - Testing of samples to be increased

- ❑ Ban for award of any conductor package for 3 years.

Thank You.

Good Morning to all of you. I would like to focus on Lokayukta bill and its provisions.

The Administrative Reforms Commission had recommended the setting up of the institution of Lokayukta for the purpose of appointment of Lokayukta at the state's level, to improve the standards of public administration, by looking into complaints against the administrative actions, including cases of corruption, favouritism and official indiscipline in administrative machinery.

One of the election promises in the election manifesto of the Janatha Party was the setting up of the Institution of the Lokayukta.

The bill provides for the appointment of a Lokayukta and one or more Upalokayuktas to investigate and report on allegations or grievances relating to the conduct of public servants.

The public servants who are covered by the Act include :-

- Chief Minister;
- all other Ministers and Members of the State Legislature;
- all officers of the State Government;
- Chairman, Vice Chairman of local authorities, Statutory bodies or Corporations established by or under any law of the State Legislature, including Co-operative Societies;
- Persons in the service of Local Authorities, Corporations owned or controlled by the State Government, a company in which not less than 50% of the shares are held by the State Government, Societies registered under the State Registration Act, Co-operative Societies and Universities established by or under any law of the Legislature.

Where, after investigation into the complaint, the Lokayukta considers that the allegation against a public servant is prima facie true and makes a declaration that the post held by him, and the declaration is accepted by the competent authority, the public servant concerned, if he is a Chief Minister or any other Minister or Member of State Legislature shall resign his office and if he is any other non-official shall be deemed to have vacated his office, and, if an official, shall be deemed to have been kept under suspension, with effect from the date of the acceptance of the declaration.

If after investigation, the Lokayukta is satisfied that the public servant has committed any criminal offence, he may initiate prosecution without reference to any other authority. Any prior sanction required under any law for such prosecution shall be deemed to have been granted.

The Vigilance Commission is abolished. But all inquiries and investigations and other disciplinary proceedings pending before the Vigilance Commission will be transferred to the Lokayukta.

There are other incidential and consequential provisions.Hence this bill.

An act to make provision for the appointment and functions of certain authorities for making enquiries into administrative action relatable to matters specified in List II or List III of the Seventh Schedule to the Constitution, taken by or on behalf of the Government of Karnataka or certain public authorities in the State of Karnataka (including any omission or commissions in connection with or arising out of such action) in certain cases and for matters connected therewith or ancillary thereto.

Whereas it is expedient to make provision for the appointment and functions of certain authorities for making enquiries into administrative action relatable to matters specified in List II or List III of the Seventh Schedule to the Constitution taken by or on behalf of the Government of Karnataka or certain public authorities in the State of Karnataka (including any Omission of commission in connection with or arising out of such action) in certain cases and for matters connected therewith or ancillary thereto:-

Be it enacted by the Karnataka Legislature in Thirty-fourth Year of the Republic of India as follows:-

1. **Short title and commencement**:-

(1) This Act may be called the Karnataka Lokayukta Act, 1984.

(2) It shall come into force on such date as the State Government may, by notification appoint.

2. **Definitions**:- In this Act, unless the context otherwise requires,-

(1) "Action" means administrative action taken by way of decision, recommendation or finding or in any other manner and includes wilful failure or omission to act and all other expressions relating to such action shall be construed accordingly;

(2) "Allegation" in relation to a public servant includes any affirmation that such public servant-

(a) has abused his position as such public servant to obtain any gain or favour to himself or to any other person or to cause undue harm or hardship to any other person;
(b) was actuated in the discharge of his functions as such public servant by personal interest or improper or corrupt motives;
(c) is guilty of corruption, favouritism, nepotism or lack of integrity in his capacity as such public servant;
OR
(d) has failed to act in accordance with the norms of integrity and conduct which ought to be followed by public servants of the class to which he belongs:

(3) "Chief Minister" means the Chief Minister of Karnataka;

(4) "Competent Authority" in relation to a public servant means-

(a) in the case of Chief Minister or a member of the State Legislature, the Governor acting in his discretion;
(b) in the case of a Minister or Secretary, the Chief Minister;
(c) in the case of a Government servant other than a Secretary, the Government of Karnataka;
(d) in the case of any other public servant, such authority as may be prescribed;

(5) "corruption" includes anything made punishable under Chapter IX of the Indian Penal Code or under the Prevention of Corruption Act, 1947;

(6) "Government Servant" means a person who is a member of the Civil Services of the State of Karnataka or who holds a civil post or is serving in connection with the affairs of the State of Karnataka and includes any such person whose services are temporarily placed at the disposal of the Government of India, the Government of another State, a local authority or any person whether incorporated or not, and also any person in the service of the Central or another State Government or a local or other authority whose services are temporarily placed at the disposal of the Government of Karnataka;

(7) "Governor" means the Governor of Karnataka;

(8) "grievance" means a claim by a person that he sustained injustice or undue hardship in consequence of mal-administration;

(9) "Lokayukta" means the person appointed as the Lokayukta under section 3;

(10) "Mal-administration" means action taken or purporting to have been taken in the exercise of administrative function in any case where,-

(a) such action or the administrative procedure or practice governing such action is unreasonable, unjust, oppressive or improperly discriminatory; or
(b) there has been wilful negligence or undue delay in taking such action or the administrative procedure or practice governing such action involves undue delay;

(11) "Minister" means a member of the Council or Ministers for the State of Karnataka, but excluding the Chief Minister;

(12) "Public servant" means a person who is or was at any time,-

(a) the Chief Minister;
(b) a Minister;
(c) a Member of the State Legislature;
(d) a Government servant;
(e) the Chairman and Vice-Chairman (by whatever name called) or a member of a local authority in the State of Karnataka or a statutory body or corporation established by or under any law of the State Legislature, including a co-operative society, or a Government Company within the meaning of section 617 of the Companies Act, 1956 and such other corporations or boards as the State Government may, having regard to its financial interest in such corporations or boards, by notification, from time to time, specify;
(f) member of a Committee or Board, statutory or non-statutory, constituted by the Government;
(g) a person in the service of pay of,-
(i) a local authority in the State of Karnataka;
(ii) a statutory body or a corporation (not being a local authority) established by or under a State or Central Act, owned or controlled by the State Government and any other board or Corporation as the State Government may, having regard to its financial interest therein by notification, from time to time, specify;
(iii) a company registered under the Companies Act, 1956, in which not less than fifty one percent of the paid up share capital is held by the State Government, or any company which is a subsidiary of such company;

(iv) a society registered or deemed to have been registered under the Karnataka Societies Registration Act, 1960, which is subject to the control of the State Government and which is notified in this behalf in the Official Gazette;
(v) a co-operative Society
(vi) a university;

Explanation- In this clause, "co-operative society" means a co-operative society registered or deemed to have been registered under the Karnataka Co-operative Societies Act, 1959, and "university" means a university established or deemed to be established by or under any law of the State Legislature;

(13) "secretary" means the Chief Secretary, an Additional Chief Secretary, an Additional Chief Secretary, a Principal Secretary, a Secretary, or a Secretary-II to the Government of Karnataka and includes a Special Secretary, an Additional Secretary and a Joint Secretary;

(14) "Upalokayukta" means a person appointed as Upalokayukta under Section 3.

3. Appointment of Lokayukta and Upalokayukta.

(1) For the purpose of conducting investigations and enquiries in accordance with the provisions of this Act, the Governor shall appoint a person to be known as the Lokayukta and one or more persons to be known as the Upalokayukta or Upalokayuktas.

(2) (a) A person to be appointed as the Lokayukta shall be a person who has held the office of a Judge of the Supreme Court or that of the Chief Justice of a High Court and shall be appointed on the advice tendered by the Chief Minister in consultation with the Chief Justice of the High Court of Karnataka, the Chairman, Karnataka Legislative Council, the Speaker, Karnataka Legislative Assembly, the Leader of the Opposition in the Karnataka Legislative Council and the Leader of the Opposition in the Karnataka Legislative Assembly.

(b) A person to be appointed as an Upalokayukta shall be a person who has held the office of the Judge of a High Court and shall be appointed on the advice tendered by the Chief Minister in consultation with the Chief Justice of the High Court of Karnataka, the Chairman, Karnataka Legislative Council, the Speaker, Karnataka Legislative Assembly, the Leader of the opposition in the Karnataka Legislative Council and the Leader of the opposition in the Karnataka Legislative Assembly.

(3) A person appointed as the Lokayukta or an Upalokayukta shall, before entering upon his office, make and subscribe before the Governor, or some person appointed in that behalf of him, an oath or affirmation in the form set out for the purpose in the First Schedule.

4. **Lokayukta or Upalokayukta not to hold any other office**- The Lokayukta or Upalokayukta shall not be a member of the Parliament or be a member of the Legislature of

any State and shall not hold any office or trust of profit (other than his office as Lokayukta or Upalokayukta) or be connected with any political party or carry on any business or practice any profession and accordingly, before he enters upon his office, a person appointed as the Lokayukta or an Upalokayukta shall-

(a) if he is a Member of the Parliament or of the Legislature of any State, resign such membership; or
(b) if he holds any office of trust or profit, resign from such office; or
(c) if he is connected with any political party, sever his connection with it; or
(d) if he is carrying on any business, sever his connection (short of divesting himself of ownership) with the conduct and management of such business; or
(e) if he is practicing any profession, suspend practice of such profession.

5. Term of office and other conditions of service of Lokayukta and Upalokayukta – (1) A person appointed as the Lokayukta or Upalokayukta shall hold office for a term of five years from the date on which he enters upon his office;

Provided that.-

(a) the Lokayukta or an Upalokayukta may, by writing under his hand addressed to the Governor, resign his office;
(b) the Lokayukta or an Upalokayukta may be removed from office in the manner provided in Section 6.

(2) On ceasing to hold office, the Lokayukta or an Upalokayukta shall be ineligible for further employment to any office of profit under the Government of Karnataka or in any authority, corporation, company, society or university referred to in item (g) of clause (12) of section 2.

(3) There shall be paid to the Lokayukta and the Upalokayukta every month a salary equal to that of the Chief Justice of a High Court and that of a Judge of the High Court respectively;

(4) The allowances payable to and other conditions of service of the Lokayukta or an Upalokayukta shall be such as may be prescribed;

Provided that.-

(a) in prescribing the allowances payable to and other conditions of service of the Lokayukta, regard shall be had to the allowances payable to and other conditions of service of the Chief Justice of India;

(b) in prescribing the allowances payable to and other conditions of service of the Upalokayukta, regard shall be had to the allowances payable to and other conditions of service of a Judge of the High Court;

(c) no Dearness Allowance shall be payable either to the Lokayukta or Upalokayukta:

Provided further that the allowances payable to and other conditions of service of the Lokayukta or Upalokayukta shall not be varied to his disadvantage of his appointment.

(5) The administrative expenses of the office of the Lokayukta and Upalokayukta including all salaries, allowances and pensions payable to or in respect of persons serving in that office, shall be charged on the Consolidated Fund of the State.

6. Removal of Lokayukta or Upalokayukta-

(1) The Lokayukta or an Upalokayukta shall not be removed from his office except by an order of the Governor passed after an address by each House of the State Legislature supported by a majority of the total membership of the House and by a majority of not less than two thirds of the members of that House present and voting has been presented to the Governor in the same session for such removal on the ground of proved misbehaviour or incapacity.

(2) The procedure of the presentation of an address and for the investigation and proof of the misbehaviour or incapacity of the Lokayukta or an Upalokayukta under sub-section (1) shall be as provided in the Judges (Inquiry) Act, 1968 in relation to the removal of a Judge and accordingly the provisions of that Act shall, mutatis mutandis, apply in relation to the removal of the Lokayukta and Upalokayukta as they apply in relation to the removal of a Judge.

7. **Matters which may be investigated by the Lokayukta and an Upalokayukta.–** (1) Subject to the provisions of this Act, the Lokayukta may investigate any action which is taken by or with the general or specific approval of,-

(a) (i) the Chief Minister;

(ii) a Minister;

(iii) a member of the State Legislature;

(iv) the Chairman and Vice-Chairman (by whatever name called) or a member of an authority, board, or a committee, a statutory or non-statutory body or

a corporation established by or under any law of the State Legislature including a society, cooperative society or a Government company within the meaning of section 617 of the Companies Act, 1956, nominated by the State Government;

in any case where a complaint involving a grievance or an allegation is made in respect of such action.

(b) any other public servant holding a post or office carrying either a fixed pay, salary or remuneration of more than rupees twenty thousand per month or a pay scale the minimum of which is more than rupees twenty thousand, as may be revised from time to time in any case where a complaint involving a grievance or an allegation is made in respect of such action or such action can be or could have been, in the opinion of the Lokayukta, recorded in writing, the subject of a grievance or an allegation.

(2) Subject to the provisions of the Act, an Upalokayukta may investigate any action which is taken by or with the general or specific approval of, any public servant not being the Chief Minister, Minister, Member of the Legislature, Secretary or other public servant refereed to in sub-section (1), in any case where a complaint involving a grievance or an allegation is made in respect of such action or such action can be or could have been, in the opinion of the Upalokayukta, recorded in writing. the subject of a grievance or an allegation.

(2A) Notwithstanding anything contained in sub-sections (1) and (2), the Lokayukta or an Upalokayukta may investigate any action taken by or with the general or specific approval of a public servant, if it is referred to him by the State Government.

(3) Where two or more Upalokayuktas are appointed under this Act, the Lokayukta may, by general or special order, assign to each of them matters which may be investigated by them under this Act.

Provided that no investigation made by an Upalokayukta under this Act, and no action taken or things done by him in respect of such investigation shall be open to question on the ground only that such investigation relates to a matter which is not assigned to him by such order.

(4) Notwithstanding anything contained in sub-sections (1) to (3), when the office of an Upalokayukta is vacant by reason of his death, resignation, retirement, removal or otherwise or when an Upalokayukta is unable to discharge his functions owing to absence, illness or any other cause, his function may be discharged by the other Upalokayukta, if any and if there is no other Upalokayukta by the Lokayukta.

8. **Matters not subject to investigation**:-

(1) Except as hereinafter provided, the Lokayukta or an Upalokayukta shall not conduct any investigation under this Act in the case of a complaint involving a grievance in respect of any action, -

(a) if such action relates to any matter specified in the Second Schedule; or

(b) if the complainant has or had, any remedy by way of appeal, revision, review or other proceedings before any tribunal, Court officer or other authority and has not availed of the same.

(2) The Lokayukta or an Upalokayukta shall not investigate, -

(a) any action in respect of which a formal and public enquiry has been ordered with the prior concurrence of the Lokayukta or an Upalokayukta, as the case may be;

(b) any action in respect of a matter which has been referred for inquiry, under the Commission of Inquiry Act, 1952 with the prior concurrence of the Lokayukta or an Upalokayukta, as the case may be;

(c) any complaint involving a grievance made after the expiry of a period of six months from the date on which the action complained against become known to the complainant; or

(d) any complaint involving an allegation made after the expiry of five years from the date on which the action complained against is alleged to have taken place:

Provided that he may entertain a complaint referred to in clauses (c) and (d) if the complainant satisfies that he had sufficient cause for not making the complaint within the period specified in those clauses.

(3) In the case of any complaint involving a grievance, nothing in this Act shall be construed as empowering the Lokayukta or an Upalokayukta to question any administrative action involving the exercise of a discretion except where he is satisfied that the elements involved in the exercise of the discretion are absent to such an extent that the discretion can prima facie be regarded as having been improperly exercised.

9. **Provisions relating to complaints and investigations**-

(1) Subject to the provisions of this Act, any person may make a complaint under this Act to the Lokayukta or an Upalokayukta.

Provided that in case of a grievance, if the person aggrieved is dead or for any reason, unable to act for himself, the complaint may be made or if it is already made, may be prosecuted by

his legal representatives or by any other person who is authorized by him in writing in this behalf.

(2) Every complaint shall be made in the form of a statement supported by an affidavit and in such forms and in such manner as may be prescribed.

(3) Where the Lokayukta or an Upalokayukta proposes, after making such preliminary inquiry as he deemed fit to conduct any investigation under this Act, he.-

(a) shall forward a copy of the complaint and in the case of an investigation initiated suo-motu by him, the opinion recorded by him to initiate the investigation under sub-section (1) or (2), as the case may be, of section 7; to the public servant and the Competent Authority concerned;
(b) shall afford to such public servant an opportunity to offer his comments on such complaint or opinion recorded under sub-section (1) and (2) of section 7 as the case may be;
(c) may make such order as to the safe custody of documents relevant to the investigation, as he deems fit.

(4) Save as aforesaid, the procedure for conducting any such investigation shall be such, and may be held either in public or in camera, as the Lokayukta or the Upalokayukta, as the case may be, considers appropriate in the circumstances of the case.

(5) The Lokayukta or the Upalokayukta may, in his discretion, refuse to investigate or cease to investigate any complaint involving a grievance or an allegation, if in his opinion,-

(a) the complaint is frivolous or vexatious or is not made in good faith;
(b) There are no sufficient grounds for investigating or, as the case may be, for continuing the investigation; or

(c) Other remedies are available to the complainant and in the circumstances of the case it would be more proper for the complainant to avail such remedies.

(6) In any case where the Lokayukta or an Upalokayukta decides not to entertain a complaint or to discontinue any investigation in respect of a complaint he shall record his reasons therefor and communicate the same to the complainant and the public servant concerned.

(7) The conduct of an investigation under this Act against a Public servant in respect of any action shall not affect such action, or any power or duty of any other public servant to take further action with respect to any matter subject to the investigation.

10. Issue of Search Warrant, etc.- (1) Wherein consequence of information in his possession, the Lokayukta or an Upalokayukta –

(a) has reason to believe that any person. –

(i) to whom a summon or notice under this Act, has been or might be issued, will not or would not produce or cause to be produced any property, document or thing which will be necessary or useful for or relevant to any inquiry or other proceeding to be conducted by him;
(ii) is in possession of any money, bullion, jewellery or other valuable article or thing and such money, bullion, jewellery or other valuable article or thing represents either wholly or partly income or property which has not been disclosed to the authorities for the purpose of any law or rule in force which requires such disclosure to be made; or

(b) considers that the purposes of any inquiry or other proceedings to be conducted by him will be served by a general search or inspection, he may by a search warrant authorize any Police officer not below the rank of an Inspector of Police to conduct a search or carry out an inspection in accordance therewith and in particular to, -

(i) enter and search any building or place where he has reason to suspect that such property, document, money, bullion, jewellery or other valuable article or thing is kept;
(i-a) search any person who is reasonably suspected of concealing about his person any article for which search should be made;
(ii) break open the lock of any door, box, locker safe, almirah or other receptacle for exercising the powers conferred by sub-clause (i) where the keys thereof are not available.
(iii) Seize any such property, document, money, bullion, jewellery or other valuable article or thing found as a result of such search;
(iv) place marks of identification on any property or document or make or cause to be made; extracts or copies therefrom; or

(v) make a note or an inventory of any such property, document, money, bullion, Jewellery or other valuable article or thing.

(2) The provisions of the Code of Criminal Procedure, 1973, relating to search and seizure shall apply, so far as may be, to searches and seizures under sub-section (1).

(3) A warrant issued under sub-section (1) shall for all purposes, be deemed to be a warrant issued by a court under section 93 of the Code of Criminal Procedure, 1973.

11. **Evidence_** (1) Subject to the provisions of this section, for the purpose of any investigation (including the preliminary inquiry, if any, before such investigation) under this Act, the Lokayukta or an Upalokayukta may require any public servant or any other person

who, in his opinion is able to furnish information or produce documents relevant to the investigation to furnish any such information or produce any such document.

(2) For the purpose of any such investigation (including the preliminary inquiry) the Lokayukta or an Upalokayukta shall have all the powers of a civil court while trying a suit under the Code of Civil Procedure, 1908 , in respect of the following matters, namely:-

(a) Summoning and enforcing the attendance of any person and examining him on oath ;
(b) Requiring the discovery and production of any document;
(c) Receiving evidence on affidavits ;
(d) Requisitioning any public record or copy thereof from any court or office ;
(e) Issuing commissions for the examination of witnesses or documents ;
(f) such other matters as may be prescribed.

(3) Any proceeding before the Lokayukta or an Upalokayukta shall be deemed to be a judicial proceeding with in the meaning of section 193 of the Indian Penal Code.

(4) No person shall be required or authorised by virtue of this Act to furnish any such information or answer any such question or produce so much of any document.

(a) as might prejudice the affairs of the State of Karnataka or the security or defence or international relations of India (including India's relations with the Government of any other country or with any international organisation);

(b) as might involve the disclosure of proceedings of the Cabinet of the State Government or any Committee of that Cabinet,and for the purpose of this sub-section, a certificate issued by the Chief Secretary certifying that any information, answer or portion of a document is of the nature specified in clause(a) or clause(b), shall be binding and conclusive.

(5) For the purpose of investigation under this Act no person shall be compelled to give any evidence or produce any document, which he could not be compelled to give or produce in proceedings before a court.

12. **Reports of Lokayukta, etc**. (1) If, after investigation of any action involving a grievance has been made, the Lokayukta or an Upalokayukta is satisfied that such action has resulted in injustice or undue hardship to the complainant or to any other person, the Lokayukta or an Upalokayukta shall, by a report in writing, recommend to the competent authority concerned that such injustice or hardship shall be remedied or redressed in such manner and within such time as may be specified in the report.

(2) The competent authority to whom a report is sent under sub-section(1) shall, within one month of the expiry of the period specified in the report, intimate or cause to be intimated to or the Lokayukta the Upalokayukta the action taken on the report.

(3) If, after investigation of any action involving an allegation has been made, the Lokayukta or an Upalokayukta is satisfied that such allegation is substantiated either wholly or partly, he shall by report in writing communicate his findings and recommendations along with the relevant documents, materials and other evidence to the competent authority.

(4) The Competent authority shall examine the report forwarded to it under sub-section (3) and within three months of the date of receipt of the report, intimate or cause to be intimated to the Lokayukta or the Upalokayukta the action taken or proposed to be taken on the basis of the report.

(5) If the Lokayukta or the Upalokayukta is satisfied with the action taken or proposed to be taken on his recommendations or findings referred to in sub-sections (1) and (3), he shall close the case under information to the complainant, the public servant and the competent authority concerned; but where he is not so satisfied and if he considers that the case so deserves, he may make a special report upon the case to the Governor and also inform the Competent Authority concerned and the Complainant.

(6) The Lokayukta shall present annually a consolidated report on the performance of his functions and that of the Upalokayukta under this Act to the Governor.

(7) On receipt of the special report under sub-section (5), or the annual report under sub-section (6), the Governor shall cause a copy thereof together with an explanatory memorandum to be laid before each House of the State Legislature.

(8) The Lokayukta or an Upalokayukta may at his discretion make available, from time to time, the substances of cases closed or otherwise disposed of by him which may appear to him to be of general, public, academic or professional interest in such manner and to such persons as he may deem appropriate.

13. Public servant to vacate office if directed by Lokayukta etc.

(1) Where after investigation into a complaint the Lokayukta or an Upalokayukta is satisfied that the complaint involving an allegation against the public servant is substantiated and that the public servant concerned should not continue to hold the post held by him, the Lokayukta or the Upalokayukta shall make a declaration to that effect in his report under sub-section (3) of section 12. Where the competent authority is the Governor, State Government or the Chief Minister, it may either accept or reject the declaration after giving an opportunity of being heard. In other cases, the competent authority shall send a copy of such report to the State Government, which may either accept or reject the declaration. If it is not rejected

within a period of three months from the date of receipt of the report, or the copy of the report, as the case may be, it shall be deemed to have been accepted on the expiry of the said period of three months.

(2) If the declaration so made is accepted or is deemed to have been accepted, the fact of such acceptance or the deemed acceptance shall immediately be intimated by Registered post by the Governor, the State Government or the Chief Minister if any of them is the competent authority and the State Government in other cases then, notwithstanding anything contained in any law, order, notification, rule or contract of appointment, the public servant concerned shall, with effect from the date of intimation of such acceptance or of the deemed acceptance of the declaration,

i) if the Chief Minister or a Minister resign his office of the Chief Minister, or Minister, as the case may be;

ii) if a public servant falling under items (e) and (f), but not falling under items (d) and (g) of clause (12) of section 2, be deemed to have vacated his office; and

iii) if a public servant falling under items (d) and (g) of clause (12) of section 2, be deemed to have been placed under suspension by an order of the appointing authority.

Provided that if the public servant is a member of an All India Service as defined in section 2 of the All India Services Act, 1951 (Central Act 61 to 1951) the State Government shall take action to keep him under suspension in accordance with the rules or regulations applicable to his service.

14. Initiation of Prosecution.- If after investigation into any complaint the Lokayukta or an Upalokayukta is satisfied that the public servant has committed any criminal offence and should be prosecuted in a court of law for such offence, then, he may pass an order to that effect and initiate prosecution of the public servant concerned and if prior sanction of any authority is required for such prosecution, then, notwithstanding anything contained in any law, such sanction shall be deemed to have been granted by the appropriate authority on the date of such order.

15. Staff of Lokayukta, etc.- (1) There shall be such officers and employees as may be prescribed to assist the Lokayukta and the Upalokayukta or the Upalokayuktas in the discharge of their functions under this Act.

(2) The categories, recruitment and conditions of service of the officers and employees referred in sub-section (1) including such special conditions as may be necessary for enabling them to act without fear in the discharge of their functions, shall be such as may be prescribed in consultation with the Lokayukta.

(3) Without prejudice to the provisions of sub-section (1), the Lokayukta or an Upalokayukta may for the purpose of conducting investigations under this Act utilize the services of.-

(a) any officer or investigating agency of the State Government; or
(aa) any officer or investigating agency of the Central Government with the prior concurrence of the Central Government and State Government; or
(b) any other person or any other agency.

(4) The officers and other employees referred to in sub-section (1) shall be under the administrative and disciplinary control of the Lokayukta:

Provided that when the office of the Lokayukta is vacant by reason of his death, resignation, retirement, removal or otherwise or when Lokayukta is unable to discharge his functions owing to absence, illness or any other cause, the Upalokayukta or if there are more than one Upalokayukta, the senior among them may discharge the functions of the Lokayukta under this sub-section.

15. Secrecy of Information- (1) Any information obtained by the Lokayukta or an Upalokayukta or members of his staff in the course of or for the purpose of any investigation under this Act and any evidence recorded or collected in connection with such information, shall be treated as confidential and no court shall be entitled to compel the Lokayukta or the Upalokayukta or any public servant to give evidence relating to such information or produce the evidence so recorded or collected.

(2) Nothing in sub-section (1) shall apply to the disclosure of any information or particulars referred to therein, -

(a) for the purpose of this Act or for the purposes of any action or proceedings to be taken on such report under section 12;
(b) for purposes of any proceedings for an offence under the Official Secrets Act, 1923, or an offence of giving or fabricating false evidence under the Indian Penal Code or for purposes of trial of any offence under section 14 or any proceedings under section 17; or
(c) for such other purposes as may be prescribed.

17. Intentional insult or interruption to or bringing into disrepute the Lokayukta or Upalokayukta.- (1) Whoever intentionally insults or causes any interruption to the Lokayukta or Upalokayukta while the Lokayukta or Upalokayukta is conducting any investigation or inquiry under this Act shall on conviction be punished with simple imprisonment for a term which shall not be less than six months but may extend to one year or with fine, or with both.

(2) Whoever, by words spoken or intended to be read, makes or publishes any statement or does any other act, which is calculated to bring the Lokayukta or an Upalokayukta into disrepute, shall, on conviction, be punished with simple imprisonment for a term which shall not be less than six months but may extend to one year or with fine, or with both.

(3) The provisions of section 199 of Code of Criminal procedure, 1973, shall apply in relation to an offence under sub-section (1) or sub-section (2) as they apply in relation to an offence referred to in sub-section (1) of the said Section 199, subject to the modification that no complaint in respect of such offence shall be made by the Public Prosecutor except with the previous sanction of the Lokayukta or the concerned Upalokayukta;

Provided that the Court may for any adequate and special reasons to be mentioned in the judgment impose a lesser sentence of imprisonment and fine.

17A. Power to punish for contempt

The Lokayukta or Upa-Lokayukta shall have, and exercise the same jurisdiction powers and authority in respect of contempt of itself as a High court has and may exercise, and, for this purpose, the provisions of the Contempt of Courts Act, 1971 (Central Act 70 of 1971) shall have the effect subject to the modification that the references therein to the High Court shall be construed as including a reference to the Lokayukta or Upalokayukta, as the case may be.

18. Protection- (1) No suit, prosecution, or other legal proceedings shall lie against the Lokayukta or an Upalokayukta or against any officer, employee, agency or person referred to in Section 15 in respect of anything which is in good faith done while acting or purporting to act in the discharge of his official duties under this Act.

(2) No proceedings of the Lokayukta or an Upalokayukta shall be held to be bad for want of form and except on the ground of jurisdiction, no proceedings or decision of the Lokayukta or an Upalokayukta shall be liable to be challenged, reviewed, quashed or called in question in any court of ordinary Civil Jurisdiction.

19. **Conferment of additional functions on Lokayukta or Upalokayukta –**

(1) The Government may, by order, in writing and after consultation with an Upalokayukta, confer on the Upalokayukta powers to hold, in such manner and through such officers, employees and agencies referred to in section 15, as may be prescribed, enquiries against Government servants and persons referred to in item (g) of clause (12) of section 2, other than those falling under clause (ii) and (iv)of sub section (1) of Section (7) in disciplinary or other proceeding transferred under sub-section (3) of Section 26 commenced in furtherance of the recommendations of the Upalokayukta or otherwise.

(2) where powers are conferred on an Upalokayukta, under sub-section (1) such Upalokayukta shall exercise the same powers and discharge the same functions as he would in the case of any investigation made on a complaint involving a grievance or an allegation, as the case may be, and the provisions of this Act shall apply accordingly.

20. Prosecution for false complaint- (1) Notwithstanding anything contained in this Act, whoever makes any false and frivolous or vexatious complaint under this Act shall, on conviction be punished with imprisonment for a term which shall not be less than six months but which may extend to three years and with fine which shall not be less than two thousand rupees but which may extend to five thousand rupees.

(2) No Court, except a Court of a Metropolitan Magistrate or a Judicial Magistrate First Class shall take cognizance of an offence under sub section (1).

(2A) No such Court shall take cognizance of an offence under sub-section (1) except on a complaint made by a person against whom false, frivolous or vexatious complaint was made after obtaining the previous sanction of the Lokayukta or the Upalokayukta, as the case may be.

(3) The prosecution in relation to an offence under sub-section (1) shall be conducted by the public prosecutor and all expenses connected with such prosecution shall be borne by the State Government.

21. Power to delegate- The Upalokayukta may, subject to such rules as may be prescribed, by general or special order, in writing direct that the functions and powers conferred by section 19 may also be exercised or discharged by such of the officers, employees or agencies referred to in section 15 as may be specified in the order.

22. Public Servants to submit property statements-

(1) Every public servant referred to in Sub-Section (1) of Section 7, other than a Government Servant, shall within three months after the commencement of this Act and thereafter before the 30th June of every year submit to the Lokayukta in the prescribed form a statement of his assets and liabilities and those of the members of his family.

(2) If no such statement is received by the Lokayukta from any such public servant within the time specified in sub-section (1), the Lokayukta shall make a report to that effect to the competent authority and send a copy of the report to the public servant concerned. If within two months of such report the public servant concerned does not submit such statement, the Lokayukta, shall publish or cause to be published the name of such public servant in three news papers having wide publication in the State.

Explanation- In this section "family of a public servant" means the spouse and such children and parents of the public servant as are dependent on him.

23. Power to make rules – (1) The State Government may, by notification in the Official Gazette, make rules for the purpose of carrying into effect the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing provisions, such rules may provide for .-

(a) the authorities to be prescribed under sub-clause (d) of clause (4) of section.2;

(b) the allowance and pensions payable to and other conditions of service of the Lokayukta and an Upalokayukta;

(c) the form and manner in which a complaint may be made;

(d) the powers of a Civil Court which may be exercised by the Lokayukta or an Upalokayukta under clause (f) of sub-section (2) of section 11;

(e) the salary, allowances, recruitment and other conditions of service of the staff and employees of the Lokayukta or Upalokayukta under sub-section (2) of section 15;

(f) enquiries against Government servants under section 19;

(g) any other matter for which rules have to be made are necessary under this Act.

2A) Any rule made under this Act may be made with retrospective effect and when such a rule is made the reasons for making the rule shall be specified in a Statement laid before both Houses of the State Legislature subject to any modification made under sub-section (3). Every rule made under this Act shall have effect as if enacted in this Act.

(3) Every rule made under this Act shall be laid as soon as may be after it is made before each House of the State Legislature while it is in session for a total period of thirty days which may be comprised in one session or in two or more successive sessions and if, before the expiry of the session in which it is so laid or the session immediately following both Houses agree in making any modification in the rule or both Houses agree that the rule should not be made, the rule shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule.

24. Removal of doubts- (1) For the removal of doubts it is hereby declared that nothing in this Act shall be construed as authorising the Lokayukta or an Upalokayukta to investigate any action which is taken by or with the approval of, -

(a) any Judge as defined in section 19 of the Indian Penal Code;

(b) any officer or servant of any civil or criminal court in India;

(c) the Accountant General for Karnataka;

(d) the Chief Election Commissioner, the Election Commissioners and the Regional Commissioners referred to in Article 324 of the Constitution and the Chief Electoral Officer, Karnataka State;

(e) the Speaker of the Karnataka Legislative Assembly or the Chairman of the Karnataka Legislative Council, and

(f) the Chairman or a member of the Karnataka Public Service Commission,

(2) The provisions of this Act shall be in addition to the provisions of any other enactment or any rule or law under which any remedy by way of appeal, revision, review or in any other manner is available to a person making a complaint under this Act in respect of any action and nothing in this Act shall limit or affect the right of such person to avail of such remedy.

25. Removal of difficulties- Notwithstanding anything contained in this Act, the Governor may, by order, make such provision as he may consider necessary or expedient, -

(i) for bringing the provisions of this Act into effective operation;

(ii) for continuing the enquiries and investigations against Government servants and persons referred to in item (g) of clause 12 of section 2 pending before the Government or any other authority including the Karnataka State Vigilance Commission constituted under the Karnataka State Vigilance Commission Rules, 1980 by the Lokayukta or an Upalokayukta.

26. Repeal and savings – (1) The Karnataka State Vigilance Commission Rules, 1980 and the Karnataka Public Authorities (Disciplinary Proceedings against Employees) Act, 1982 (Karnataka Act 31 of 1982) and the Karnataka Lokayukta Ordinance, 1984 (Karnataka Ordinance 1 of 1984) are hereby repealed.

(2) Notwithstanding such repeal any act or thing done under the said rules or Act or Ordinance shall be deemed to have been done under this Act and may be continued and completed under the corresponding provisions of this Act.

(3) All enquiries and investigations and other disciplinary proceedings pending before the Karnataka State Vigilance Commission constituted under the Karnataka State Vigilance Commission Rules, 1980 and which have not been disposed of, shall stand transferred to and be continued by the Upalokayukta as if they were commenced before him under this Act.

(4) Notwithstanding anything contained in this Act, initially the staff of the Lokayukta shall consist of the posts of the Secretary and other Officers and Employees of the Karnataka

State Vigilance Commission constituted under the Karnataka State Vigilance Commission Rules, 1980, immediately before the commencement of this Act and appointments to the said posts are hereby made by the transfer of the Secretary and other officers and employees of the State Vigilance Commission holding corresponding posts. The salaries, allowances and other terms and conditions of services of the said Secretary, officers and other employees shall, until they are varied, be the same as to which they were entitled to immediately before the commencement of this Act.

FIRST SCHEDULE

[See Section 3 (3)]

I, …… having been appointed as Lokayukta/ Upalokayukta do swear in the name of God solemnly affirm that I will bear true faith and allegiance to the Constitution of India as by law established and I will duly and faithfully and to the best of my ability, knowledge and Judgment perform the duties of my office without fear or favour, affection or ill-will.

SECOND SCHEDULE

[See Section 8(i)(a)]

(a) Action taken for the purpose of investigating crimes relating to the security of the State

(b) Action taken in the exercise of powers in relation to determining whether a matter shall go to a court or not,

(c) Action taken in matters which arise out of the terms of a contract governing purely commercial relations of the administration with customers or suppliers except where the complainant alleges harassment or gross delay in meeting contractual obligations.

(d) Action taken in respect of appointments, removals, pay, discipline, superannuation or other matters relating to conditions of service of public servants but not including action relating to claims for pension, gratuity, provident fund or to any claims which arise on retirement, removal or termination of service.

(e) Grant of honours and awards.

Thank You.

Welcome back. I hope the lunch was great. Till there is some issue kindly let us know if any change in the diet is required. I was just going to say that I had a complain that the lunch was very good. That is why we have one session after lunch so that everyone can at **least** withhold sleep for one hour. it is the self directed learning and sometimes

we learn in our sleep also. Maybe we can take from you and ask the manager hospitality to see the changes required in the lunch. We're going to have one course on stress management, in that we could discuss what food suits are working condition. In Bombay we have working lunch or working meal which basically consist of light food so that one is not induced to sleeping. I have organised a movie for you tomorrow. Can u arrange for talwar. We will check with the protocol and let you know. I'm sure you all will like the movie we are showing i.e. prayer for rain. It is day after tomorrow and you all will like, it is based on economic crime and it is based on Bhopal gas leak disaster. It is an English movie, Hollywood production based on Bhopal gas leak tragedy. It is amazing movie, one thing that I liked about the movie was that it is very objective. Seriously, I have never seen such an objective piece of cinema. People do take sides, are biased but in this cinema it is a very objective presentation of the event. You are right that talvar is also very good movie but it is not based on economic crime. When an administration changes everyone starts redoing the same thing in different manner. We don't want to follow our predecessors view and want to do things on our own way. It is more on investigations side as how two different investigation team think differently and,come to different conclusion, how they interact differently, it is really an amazing movie. I cannot show that movie here as it will be caught in a piracy problem. You work on the logistics and let us know. There is a show on 7.50, I'll check if the tickets are available and also the show timings and will send somebody for necessary formalities so that you all can go and watch the movie. It is a great idea, you submit the money with somebody and they will arrange for the same. It will be done by Mr. Kulkarni. Tomorrow the show timings may change. In box there are only six seats for 350 each but you are more in number.. Library and computer is self directed learning, nobody is there to see you if you want to read in the library you can, if you want to issue a book and read in your room, it is your choice. Movie can be arranged today, let me know as you want. We will arrange last row seats. We are 13, so tomorrow 13 seats ok. We will meet at 330 for movie decision. Now let's give a chance to miss Nappinai, she will think we're in fox studio. I am just disappointed that I will not be able to join tomorrow as I have to leave today only. Movie are very educating, in fact in my presentation I will be advocating to watch many movies for a learning experience.

1. I will keep my introduction we short, I'm from Chennai, was there for 10 years started as a criminal lawyer and then moved to Bombay High Court, have been working for 15 years so it is almost 25 years of practice as an advocate. I first try that my presentation doesn't lead you to sleep. Firstly I'm

going to stand here and secondly I've liked the session to be interactive. I'm completely comfortable if you stop me midway to ask questions and put your queries. My only request is that in interaction we keep it to question and answer session and not discussion. We will give the discussion for the last slot. Since I'm addressing the High Court judges, I have formulated a presentation in such a fashion that I not only give the essence of cybercrime but also the interpretation of the cyber laws. And how the laws are evolving currently in India with the changing trends and also the geology of the law. This is the way I have structured it and one deviation that I'll be doing is from the perspective of practical application of law. I will explain how particular kind of case can be interpreted. I will start with the investigation to the discussion stage therefore the deviation is on electronic kind of evidence. That is the bread crumb train. In the morning, one of the speakers was talking why e-tenders are important, how to go about it and in one instance one software bug was introduced to favour one of the participating tender person. The very fact that they were able to trace out the software bug shows that there is always a possibility of invasion. Once you find that somebody is misusing the system you have methodology to find out the misuse. Except for some instance where there was a conscious decision that they could not be traced out, they were found by the cyber experts. In other instances you will be able to find out. I will be giving you the pointers in terms of electronic evidence. It was very interesting that Justice Mr Hegde was the speaker before me and he has already highlighted the first principle that is we are here to Justice how best we can do the Justice and putting the slides and quickly go through. What is cybercrime really rightly so India has not defined cybercrime till now, because it is a dynamic and evolving process. Every time you think that you have find a solution, they come up with new ways of committing crime, the profile of a cyber criminal as opposed to a traditional criminal or a regular criminal is that he is very educated and knowledgeable. The reason I'm saying that is that the hacker are mostly teenagers, they are not completed their school or graduation. It is not only the knowledge that distinguishes them but there command over the field. Therefore they are group of persons who know what they are actually doing. One of the earlier speaker talked about fraud pyramid, as how they give justification for the crimes committed. Thereby the cyber criminal fall in the category of sophisticated criminals/ferons. Firstly they don't know what they are doing is a crime. In the case of data theft, in case of commercial data thefts it is usually

done by former employees, invariably every data theft in the organisation is done by an employee whose relations have got sour, a disgruntled employee whose relation with a former employee has gone wrong. Most of these persons who are taking away the data don't know that they are committing a crime so awareness is not there. Secondly the law is so convoluted that the person committing the crime goes away without any punishment. By the time anyone figures out what is said in the law, even the lawyers and judges find it difficult to interpret. I'd like to point out what provision which is into the law and it has not been taken up in any case for the interpretation. As I told you cybercrime is not defined in India not all jurisdictions have shied away from this. One of the simplest definition in India is by Kerala government where it has issued a circular saying that crime is committed by using a computer or where the computer is a victim or the computer is the weapon of the crime. South Africa..... Officers against nation..... I generally don't read from the slides, I will be circulating latter on.. What is a remedy and what is the crime that we are trying to find. The world is going very fast with the way the crime is evolving. But Law has not kept pace, even with the trends which has already evolved. So we get our IT act in 2000 and before that there were highly publicised instances of virus attack. One which was very famous was with the tagline I love you virus it was sometime around March 2000. It eminated from phillipene and it hit the cyber world causing the loss of several billion. Yet the IT act came here in 2000 whereby a virus attacks is with the civil penalty under section 43. It does not categorise virus attack or the hacking or denial of service or data thefts as Civil violations or criminal acts. It took 2008 amendment to categorise them as criminal offences. One there is a vacuum and second there is lack of understanding in the application of these laws. This is a indicator list and not an exhaustive list for all the cyber crimes committed. Further I will give examples of what we have missed out and they way we have misapplied the laws. I will broadly categorise the offences against nation body and property. These were primary additions made to IT act. I will quickly run through these presentations, to section 43 and 66 and its misapplication . Now we have very well worded principle for how legislation should be drawn. Despite that it is not only section 66 a which have been stuck down due to the fallacies of bad drafting. I would like to point out two provisions which are still on the books. Which suffers from serious error of legislative drafting and unfortunately it has got a kind of legal sanction in Shreya Singhal's case which is of deep concern today. Let's look

at section 66, IT act 2000 contains very limited provisions. Firstly the cybercrime was not restricted to IT act only IPC act was also amended to include cybercrime,like forgery. IT act ten provisions were included. It gave an indication that all the cybercrime are addressed to but it was not so. Section 66 as it stood in 2000 was titled hacking which was very misleading because it said that if anybody deletes destroys or alters residing in the computer resource or residing in , happens then it is hacking but it is not the understanding of the common point of hacking, it is basically unauthorised use of computers. If you look at 66 which was originally section 43, and the first subclause a talk about hacking as we understood. In 2008 amendment section 66 was deleted and any act under section 43 is done with dishonest and fraudulent means or intent, then it will become criminal offence under 66. Mens rea was added, but that was not the problem, the problem is that the old section 66 was added as I to 43. Thereby by reverse application this was brought back in section 66. From 2000 to 2008 there was a lot of anguish the way section 66 was worded. Two draft amendment bill was circulated 2005 and 2006. In those amendment the report was submitted that section 66 would be scrapped. The government incorporated that and put it on the website for public reactions. After the Mumbai attacks what we have is a knee-jerk reaction. within a month of Mumbai attacks whatever was discussed was put on the paper. This was a mismatch and a transposition was Happened and you will find it here. Whoever destroys deletes or alters the information or diminishes its value is utility or its value was under cybercrime. The latter part which I have not said is the most the dangerous part. There was no actus reus, what it read earlier was the same way. The distinction between data and information was that the data could be in public domain in our mind or somewhere else. What should be really protected is the process data processing information but here the word used is information. Last three words does not give the actus reus but still the cybercrime is committed. And there are already instances of abuse of this section. Where company used to file litigation saying I support X number of crores of losses and it falls under section 66 thereby u should initiate action. In the provision instead of or there should be and. And is what should have been there in the provision to make it more effective. In one line there are six offences. United States also have a similar jurisdiction, it has the federal structure thereby each state has its own legislation on cybercrime. At least 15 states have this provision, SriLanka and Australia have these provisions. It is not something which is new but the

additional part which they have done here is the diminishing part because if you look at it all the legislation have delete destroy or alters part and unfortunately there is some concern with the Shreya Singhals case because that judgement relies on section 66. This is a evolving field and I guess at some point of time when it will come for the interpretation it will be done. This is misused a lot because everytime an employee leaves the employer for another organisation he is charged with data thefts. In one stance the company issued a notice to its legal head saying that when you left the company you have deleted lot of heavy fines. If I go back to Kartar Singh case the person should know that what he's doing is wrong. The fraud triangle shown in the morning by Mr Jain, one of the ground was rationalisation, rationalisation also carries with it lack of awareness in my opinion. When someone knows that something is wrong as a part of his education the chances that he will desist from doing a crime is higher, for that he must know that it is a crime. How you can say that this text matches with this kind of wording of the provisions. If I diminish the value of information residing in a computer resource I will be held liable if I have done it dishonestly or fraudulently. To diminish the value I process the information in the manner which could actually diminish the value of the information. That actus has to be clearly defined otherwise it will be left in the hands of police and judges to decide or to interpret for the right meaning of the offence. There is a hacking with actus reus. If there is a separate provision as J K then it would have served the purpose. Hacking is under the same section 43. When a case is registered it is for you to go for quashing or give it a different meaning or interpretation. section 66 covers data thefts hacking denial of service attack denial of virus attack. H is another curious addition.section 65 days with stealing distorted or changing the source code in a computer resource. The distinction between section 65 and H is that here it talked about destroying or deleting computer source code. The plagiarism of provisions is not considered a copyright violation so we are happy to plagiarise. Here we have gone one step further in plagiarism by copying our own provisions. If u read 65 and H you will find the similarity, it took me three readings to come to distinction between the two.Section 65 says of stealing the source code residing in the computer and H top of stealing the information residing in the computer. This has been very vaguely put in. There is a mens rea in section 65 and stealing of source code. One is what runs the computer and other is what is residing in the computer, that the distinction I was trying to point out. Look at some of the cases that

have come up and what has been there in those cases. Recently Sony Corporation Private Limited faced this problem and this is a scary picture of a skeleton which was put up by them for crimes committed by the hacker. What they did was, South Koreans are believed to have done this, actually Sony was about to release a movie Interview. This movie was hacked by South Koreans before it's actually being released. And Sony Corporation Private Limited were forced to release this on Internet. The hackers not only took away the propriety content but also took away the financials, the hackers said that if you release the movie we will release your data in the public domain. Sony Corporation Private Limited which plan for limited release in the theaters were forced to release this on public domain. Then there was this case of Hillary Clinton and data theft. With many applications that we download in our mobile, it comes with the package of inherent problems. Government of India is the most susceptible destination for hackers. And I met this boy of 17 years of age in New York and on the international platform he was explaining how he had hacked many of the Pakistan government sites not only he but there are many people in this age group who have been doing this successfully and efficiently. I advised him not to make such confessions as it will lead him into criminalisation. In Hillary Clinton case she was running a parallel server in the name of security, maybe with good intentions but it was hacked and all the data was stolen. She was not allowed to move the government files into any another server she claimed that maintaining a parallel server was with an honest intention of security, maybe she was right but there occurred a data there occurred the data theft. There were deported attempts of data thefts on Hillary Clinton server but none were able to breach the security measures. But the bottom line is although she was not allowed to maintain a balance of server, she maintained a parallel server. What do government officials in India do, there is this instance of 2011 whereby all the government sites were hacked, not only this, all the emails pertaining to troop movement on Indo-tibetaian border was hacked giving a dangerous breach to the security of the country . This news didn't hit the newspaper there was one headline outside the India regarding this. The reason that it was easy to hack into all his government sites was that all government officials were using Gmail account. This is absolute reverse of Hillary Clinton's case. There is this concept of trolling whereby they keep track of the contents of the email and accordingly they make targeted advertisement. In Madras High Court one of the Google case was brought regarding data tracking and Bharat

matrimonial case. The judgement was limited as it dealt with only that aspect only, otherwise this was basically the case of trolleyiny whereby they keep a track of or a trail of email or the communications made. And this they are not doing without our consent, in fact we have given them the concept of doing so without knowing by agreeing to their terms and conditions. The European Court of Justice as struk down the safe harbor concept. Under this concept they propounded that they have inherent right for cross-border transfers of information and data. This fundamental principle Google Twitter and Facebook used to trail our communication and process it accordingly. Things which you don't think were relevant are captured by them and are utilised by them for the purposes of development of the business. They analyse which customer is using what information in what manner. This fall thing of Google sync that we do, every time I book a ticket reminds me in the morning when my flight is in the fight when it is to be boarded landed etc etc. There is no concept of privacy as such. Even in United States they have very stringent laws of privacy, that is you cannot waive your right to privacy you might see on some of the sites by signing in they say you are submitting your rights to privacy. Like when you buy smart phone it says that you will not be able to assess your emails or use other applications until you sign in and in doing so you give them right of privacy. An example is of trucaller, whereby in the guise of safety or security they take away rights of privacy. It was a data aggregator. When you download it in your mobile you agree to give them the access of all the data on your mobile. They collect all the data and inform you when a new no. Calls u as they collected data from various mobiles. It aggregates all the data in bank that is the data bank's once your name or number is there your privacy is over. There was this advertisement of we care whereby Kareena Kapoor was the face of that, what it actually did was it used to keep a track of every single place that you are going to. You will be surprised to know that data is a bigger market than drugs. And the underworld loves it because it is a market to deal with. Our data is all out their that we wanted it or not. Unfortunately we put the everything on the Facebook, it is too late to remove it because they have already saved it. But more to boast about our children the post everything on the Facebook and Has become a good tool in the hands of child kidnappers. The most dangerous application is free download of games, you actually give asses to all the data in your mobile. In the case of Facebook Microsoft, in the guise of upgrading your system weather you want it or not it is forced in your system and all your data

is taken up without you realising or knowing that it is taking away all your rights of privacy. Without your permission the upgrades are pushed into your system with all the bugs which are still to be resolved by the company. There are many international laws which stops this but in India we don't have any such legislation. And whatever little law we have suffers the problems of enforcement. Hacking these days are very interrelated, please watch this movie net and net 2.0 in a visual representation of hacking, identity theft and other problems and it is very easy to follow there is this another movie the girl with golden tattoo which is also based on hacking. The movie net is very good in depicting how hacking takes place. Nowadays even the word document can contain viruses. I will show you a demo explaining this. The Wi-Fi is also one of the mode of virus transfer through piggy bank. Or if someone has hacked into the router, he will be able to see anything and everything that you. So the simple solution is that sensitive data should never be assessed through Wi-Fi. This is a viral mail that I received, fortunately it was not installed on my computer, I will try to tell you what are the three ways by which you can know that the mail sent is a genuine mail, the scary part is that you get such fictitious mail from income tax Department saying about some taxes. Now if you look at this mail which I received on my email address appears to be from Apple which mentions my Apple ID and is asking for further particulars of ID, this shows that someone has assessed my Apple account from different locations and if I have not that my registration then I'm supposed to do it now giving out my particulars. If you look at the header part it appears to be as it has been sent from Apple but the mail ID through which this has been sent carrying the name of a person's Beckman. Even I just clicking this you invite the viruses to be downloaded in your computer and then all your privacy is gone and all your data can be assessed by a third party intruder. The virus is not linked with the mail only but the scary part is that if you look at this gray line it has embedded link which means that if you reply or just click this mail all your data will be gone in the hands of a third party sitting somewhere in the world. This embedded link might lead to downloading of Trozen virus. If you see this kind of mail immediately delete that or if u download the attachment the viruses will come in your computer and even if you delete it, it will stay in your computer, once the damage is done, its done. Thereby if u see such mails with innocuous address or mail saying u have won such lakh of rupees or billions of dollars, never open it

nor download its attachment, because its downloading will cause permanent damage.

Corporate Accounting Fraud: A Case Study of Satyam Computers Limited

ABSTRACT

From Enron, WorldCom and Satyam, it appears that corporate accounting fraud is a major problem that is increasing both in its frequency and severity. Research evidence has shown that growing number of frauds have undermined the integrity of financial reports, contributed to substantial economic losses, and eroded investors' confidence regarding the usefulness and reliability of financial statements. The increasing rate of white-collar crimes demands stiff penalties, exemplary punishments, and effective enforcement of law with the right spirit. An attempt is made to examine and ana- lyze in-depth the Satyam Computer's "creative-accounting" scandal, which brought to limelight the importance of "ethics and corporate governance" (CG). The fraud committed by the founders of Satyam in 2009, is a testament to the fact that "the science of conduct is swayed in large by human greed, ambition, and hunger for power, money, fame and glory". Unlike Enron, which sank due to "agency" problem, Satyam was brought to its knee due to 'tunneling' effect. The Satyam scandal highlights the importance of securities laws and CG in 'emerging' markets. Indeed, Satyam fraud "spurred the government of India to tighten the CG norms to prevent recurrence of similar frauds in future". Thus, ma- jor financial reporting frauds need to be studied for "lessons-learned" and "strategies-to-follow" to reduce the incidents of such frauds in the future.

1. Introduction

1.1. What Is Fraud?

Fraud is a worldwide phenomenon that affects all conti- nents and all sectors of the economy. Fraud encompasses a wide-range of illicit practices and illegal acts involving intentional deception, or misrepresentation. According to the Association of Certified Fraud Examiners (ACFE), fraud is "a deception or misrepresentation that an indi- vidual or entity makes knowing that misrepresentation could result in some unauthorized benefit to the individ- ual or to the entity or some other party" [1]. In other words, mistakes are not fraud. Indeed, in fraud, groups of unscrupulous individuals manipulate, or influence the activities of a target business with the intention of mak- ing money, or obtaining goods through illegal or unfair means. Fraud cheats the target organization of its legiti- mate income and results in a loss of goods, money, and even goodwill and reputation. Fraud often employs ille- gal and immoral, or unfair means. It is essential that or-

ganizations build processes, procedures and controls that do not needlessly put employees in a position to commit fraud and that effectively detect fraudulent activity if it occurs. The fraud involving persons from the leadership level is known under the name "managerial fraud" and the one involving only entity's employees is named "fraud by employees' association".

1.2. Magnitude of Fraud Losses: A Glimpse

Organizations of all types and sizes are subject to fraud. On a number of occasions over the past few decades, major public companies have experienced financial re- porting fraud, resulting in turmoil in the capital markets, a loss of shareholder value, and, in some cases, the bankruptcy of the company itself. Although, it is gener- ally accepted that the Sarbanes-Oxley Act has improved corporate governance and decreased the incidence of fraud, recent studies and surveys indicate that investors and management continue to have concerns about finan- cial statement fraud. For example:

The ACFE's "2010 Report to the Nations on Occupa- tional Fraud and Abuse" [1] found that financial statement fraud, while representing less than five percent of the cases of fraud in its report, was by far the most costly, with a median loss of $1.7 million per incident. Survey participants estimated that the typical organization loses 5% of its revenues to fraud each year. Applied to the 2011 Gross World Product, this figure translates to a potential projected annual fraud loss of more than $3.5 trillion. The median loss caused by the occupational fraud cases in our study was $140,000. More than one-fifth of these cases caused losses of at least $1 million. The frauds re- ported to us lasted a median of 18 months before be- ing detected.

"Fraudulent Financial Reporting: 1998-2007", from the Committee of Sponsoring Organizations of the Treadway Commission (the 2010 COSO Fraud Re- port) [2], analyzed 347 frauds investigated by the US Securities and Exchange Commission (SEC) from 1998 to 2007 and found that the median dollar amount of each instance of fraud had increased three times from the level in a similar 1999 study, from a median of $4.1 million in the 1999 study to $12 mil- lion. In addition, the median size of the company in- volved in fraudulent financial reporting increased ap- proximately six-fold, from $16 million to $93 million in total assets and from $13 million to $72 million in revenues.

A "2009 KPMG Survey" [3] of 204 executives of US companies with annual revenues of $250 million or more found that 65 percent of the respondents con- sidered fraud to be a significant risk to their organiza- tions in the next year, and more than one-third of those identified financial reporting fraud as one of the highest risks.

Fifty-six percent of the approximately 2100 business professionals surveyed during a "Deloitte Forensic Center" [4] webcast about reducing fraud risk pre- dicted that more financial statement fraud would be uncovered in 2010 and 2011 as compared to the pre- vious

three years. Almost half of those surveyed (46 percent) pointed to the recession as the reason for this increase.

According to "Annual Fraud Indicator 2012" con- ducted by the National Fraud Authority (UK) [5], "The scale of fraud losses in 2012, against all victims in the UK, is in the region of £73 billion per annum. In 2006, 2010 and 2011, it was £13, £30 and £38 billions, respectively. The 2012 estimate is significantly greater than the previous figures because it includes new and improved estimates in a number of areas, in particular against the private sector. Fraud harms all areas of the UK economy".

Moreover, financial statement fraud was a contributing factor to the recent financial crisis and it threatened the efficiency, liquidity and safety of both debt and capital markets [6]. Furthermore, it has significantly increased uncertainty and volatility in financial markets, shaking investor confidence worldwide. It also reduces the cred- itability of financial information that investors use in investment decisions. When taking into account the loss of investor confidence, as well as, reputational damage and potential fines and criminal actions, it is clear why financial misstatements should be every manager's worst fraud-related nightmare [7].

1.3. Who Commits Frauds?

Everyday, there are revelations of organizations behaving in discreditable ways [8]. Generally, there are three groups of business people who commit financial state- ment frauds. They range from senior management (CEO and CFO); mid- and lower-level management and organ- izational criminals [9]. CEOs and CFOs commit ac- counting frauds to conceal true business performance, to preserve personal status and control and to maintain per- sonal income and wealth. Mid- and lower-level employ- yees falsify financial statements related to their area of responsibility (subsidiary, division or other unit) to con- ceal poor performance and/or to earn performance-based bonuses. Organizational criminals falsify financial sta- tements to obtain loans, or to inflate a stock they plan to sell in a "pump-and-dump" scheme. While many chan- ges in financial audit processes have stemmed from fi- nancial fraud, or manipulations, history and related re- search repeatedly demonstrates that a financial audit simply cannot be relied upon to detect fraud at any sig- nificant level.

1.4. Consequences of Fraudulent Reporting

Fraudulent financial reporting can have significant con- sequences for the organization and its stakeholders, as well as for public confidence in the capital markets. Pe- riodic high-profile cases of fraudulent financial reporting also raise concerns about the credibility of the US fi- nancial reporting process and call into question the roles of management, auditors, regulators, and analysts, among others. Moreover, corporate fraud impacts organizations in several areas: financial, operational and psychological [10]. While the monetary loss owing to fraud is signifi- cant, the full impact of fraud on an organization can be staggering. In fact, the losses to reputation, goodwill, and customer relations can be devastating. When fraudulent financial

reporting occurs, serious consequences ensue. The damage that result is also widespread, with a some- times devastating “ripple” effect [6]. Those affected may range from the “immediate” victims (the company’s stockholders and creditors)

to the more “remote” (those harmed when investor confidence in the stock market is shaken). Between these two extremes, many others may be affected: “employees” who suffer job loss or dimin- ished pension fund value; “depositors” in financial insti- tutions; the company’s “underwriters, auditors, attorneys, and insurers”; and even honest “competitors” whose reputations suffer by association.

As fraud can be perpetrated by any employee within an organization or by those from the outside, therefore, it is important to have an effective “fraud management” program in place to safeguard your organization’s assets and reputation. Thus, prevention and earlier detection of fraudulent financial reporting must start with the entity that prepares financial reports. Given the current state of the economy and recent corporate scandals, fraud is still a top concern for corporate executives. In fact, the sweeping regulations of Sarbanes-Oxley, designed to help prevent and detect corporate fraud, have exposed fraudulent practices that previously may have gone un- detected. Additionally, more corporate executives are paying fines and serving prison time than ever before. No industry is immune to fraudulent situations and the nega- tive publicity that swirls around them. The implications for management are clear: every organization is vulner- able to fraud, and managers must know how to detect it, or at least, when to suspect it.

2. Review of Literature

Starting in the late 1990s, a wave of corporate frauds in the United States occurred with Enron’s failure perhaps being the emblematic example. Jeffords [11] examined 910 cases of frauds submitted to the “Internal Auditor” during the nine-year period from 1981 to 1989 to assess the specific risk factors cited in the Treadway Commis- sion Report. He concluded that “approximately 63 per- cent of the 910 fraud cases are classified under the inter- nal control risks”. In addition, Smith [12] offered a “ty- pology” of individuals who embezzle. He indicated that embezzlers are “opportunist’s type”, who quickly detects the lack of weakness in internal control and seizes the opportunity to use the deficiency to his benefit. Similarly, Ziegenfuss [13] performed a study to determine the amount and type of fraud occurring in “state and local” governments. His study revealed that the most frequently occurring types of fraud are misappropriation of assets, theft, false representation; and false invoice.

On the other hand, Haugen and Selin [14] in their study discussed the value of “internal” controls, which depends largely on management’s integrity and the ready availability of computer technology, which assisted in the commitment of crime. Sharma and Brahma [15] em- phasized on “bankers” responsibility on frauds; bank frauds could crop-up in all spheres of bank’s dealing. Major cause for perpetration of fraud is laxity in obser- vance in laid-down system and procedures by supervis- ing staff. Harris and William [16], however, examined the reasons for “loan” frauds in banks and emphasized on due diligence program. Beirstaker, Brody, Pacini [17] in their study proposed numerous fraud protection and de- tection techniques. Moreover, Willison [18] examined the causes that led to the breakdown of “Barring” Bank. The

collapse resulted due to the failures in management, financial and operational controls of Baring Banks.

Choo and Tan [19] explained corporate fraud by relat- ing the "fraud-triangle" to the "broken trust theory" and to an "American Dream" theory, which originates from the sociological literature, while Schrand and Zechman [20] relate executive over-confidence to the commitment of fraud. Moreover, Bhasin [21] examined the reasons for "check" frauds, the magnitude of frauds in Indian banks, and the manner, in which the expertise of internal auditors can be integrated, in order to detect and prevent frauds in banks by taking "proactive" steps to combat frauds. Chen [22] in his study examined "unethical" lead- ership in the companies and compares the role of unethi- cal leaders in a variety of scenarios. Through the use of computer simulation models, he shows how a combina- tion of CEO's narcissism, financial incentive, sharehold- ers' expectations and subordinate silence as well as CEO's dishonesty can do much to explain some of the findings highlighted in recent high-profile financial ac- counting scandals. According to a research study performed by Cecchini *et al.* [23], the authors provided a methodology for detecting "management" fraud using basic financial data based on "support vector machines".

From the above, it is evident that majority of studies were performed in developed, Western countries. How- ever, the manager's behavior in fraud commitment has been relatively unexplored so far. Accordingly, the ob- jective of this paper is to examine managers' unethical behaviors in Satyam Computer Limited, which constitute an ex-post evaluation of alleged or acknowledged fraud case. Unfortunately, no study has been conducted to ex- amine behavioral aspects of manager's in the perpetua- tion of corporate frauds in the context of a developing economy, like India. Hence, the present study seeks to fill this gap and contributes to the literature.

3. Research Methodology, Objectives and Sources of Information

Financial reporting practice can be developed by refer- ence to a particular setting in which it is embedded. Therefore, "qualitative" research could be seen useful to explore and describe fraudulent financial reporting prac- tice. Here, two issues are crucial. First, to understand why

and how a "specific" company is committed to fraudulent financial reporting practice an appropriate "interpretive" research approach is needed. Second, case study con- ducted as part of this study, looked specifically at the largest fraud case in India, involving Satyam Computer Services (Satyam). Labelled as "India's Enron" by the Indian media, the Satyam accounting fraud has compre- hensively exposed the failure of the regulatory oversight mechanism in India. No doubt, to design better accounting systems, we need to understand how accounting systems operate in their social, political and economic contexts. The main objectives of this study are to: 1) highlight the Satyam Computers Limited's accounting scandal by por- traying the sequence of events, the aftermath of events, the key parties involved, and major follow-up actions under- taken in India; and 2) what lesions can be learned from Satyam scam?

To complement prior literature, we examined docu- mented behaviors in cases of Satyam corporate scandal, using the evidence taken from press articles, and also applied a "content" analysis to them. In terms of infor- mation collection "methodology", we searched for evi- dence from the press coverage contained in the "Factiva" database. Thus, present study is primarily based on "sec- ondary" sources of data (EBSCO host database) gathered from the related literature published in the journals, newspaper, books, statements, reports. However, as stated earlier, the nature of study is "primarily qualita- tive, descriptive and analytical".

4. Corporate Accounting Scandal at Satyam Computer Services Limited: A Case Study of India's Enron

Ironically, Satyam means "truth" in the ancient Indian language "Sanskrit" [24]. Satyam won the "Golden Pea- cock Award" for the best governed company in 2007 and in 2009. From being India's IT "crown jewel" and the country's "fourth largest" company with high-profile customers, the outsourcing firm Satyam Computers has become embroiled in the nation's biggest corporate scam in living memory [25]. Mr. Ramalinga Raju (Chairman and Founder of Satyam; henceforth called "Raju"), who has been arrested and has confessed to a $1.47 billion (or Rs. 7800 crore) fraud, admitted that he had made up profits for years. According to reports, Raju and his brother, B. Rama Raju, who was the Managing Director, "hid the deception from the company's board, senior managers, and auditors". The case of Satyam's account- ing fraud has been dubbed as "India's Enron". In order to evaluate and understand the severity of Satyam's fraud, it is important to understand factors that contributed to the "unethical" decisions made by the company's executives. First, it is necessary to detail the rise of Satyam as a competitor within the global IT services market-place. Second, it is helpful to evaluate the driving-forces behind Satyam's decisions: Ramalinga Raju. Finally, attempt to learn some "lessons" from Satyam fraud for the future.

4.1. Emergence of Satyam Computer Services Limited

Satyam Computer Services Limited was a "rising-star" in the Indian "outsourced"

IT-services industry. The com- pany was formed in 1987 in Hyderabad (India) by Mr. Ramalinga Raju. The firm began with 20 employees and grew rapidly as a "global" business. It offered IT and business process outsourcing services spanning various sectors. Satyam was as an example of "India's growing success". Satyam won numerous awards for innovation, governance, and corporate accountability. "In 2007, Ernst & Young awarded Mr. Raju with the 'Entrepreneur of the Year' award. On April 14, 2008, Satyam won awards from MZ Consult's for being a 'leader in India in CG and accountability'. In September 2008, the World Council for Corporate Governance awarded Satyam with the 'Global Peacock Award' for global excellence in corpo- rate accountability" [26]. Unfortunately, less than five months after winning the Global Peacock Award, Satyam became the centerpiece of a "massive" accounting fraud.

By 2003, Satyam's IT services businesses included 13,120 technical associates servicing over 300 customers worldwide. At that time, the world-wide IT services market was estimated at nearly $400 billion, with an es- timated annual compound growth rate of 6.4%. "The markets major drivers at that point in time were the in- creased importance of IT services to businesses world- wide; the impact of the Internet on eBusiness; the emer- gence of a high-quality IT services industry in India and their methodologies; and, the growing need of IT ser- vices providers who could provide a range of services". To effectively compete, both against domestic and global competitors, the company embarked on a variety of multi-pronged business growth strategies.

From 2003-2008, in nearly all financial metrics of in- terest to investors, the company grew measurably. Sat- yam generated USD $467 million in total sales. By March 2008, the company had grown to USD $2.1 bil- lion. The company demonstrated "an annual compound growth rate of 35% over that period". Operating profits averaged 21%. Earnings per share similarly grew, from $0.12 to $0.62, at a compound annual growth rate of 40%. Over the same period (2003-2009), the company was trading at an average trailing EBITDA multiple of 15.36. Finally, beginning in January 2003, at a share price of 138.08 INR, Satyam's stock would peak at 526.25 INR—a 300% improvement in share price after nearly five years. Satyam clearly generated significant corporate

growth and shareholder value. The company was a lead- ing star—and a recognizable name—in a global IT marketplace. The external environment in which Satyam operated was indeed beneficial to the company's growth. But, the numbers did not represent the full picture. The case of Satyam accounting fraud has been dubbed as "India's Enron".

4.2. Mr. Ramalinga Raju and the Satyam Scandal

On January 7, 2009, Mr. Raju disclosed in a letter (see **Annexure**) to Satyam Computers Limited Board of Di- rectors that "he had been manipulating the company's accounting numbers for years". Mr. Raju claimed that he overstated assets on Satyam's balance sheet by $1.47 billion. Nearly $1.04 billion in bank loans and cash that the company claimed to own was non-existent. Satyam also underreported liabilities on its balance sheet. Satyam overstated income nearly every quarter over the course of several years in order to meet analyst expectations. For example, the results announced on October 17, 2009 overstated quarterly revenues by 75 percent and profits by 97 percent. Mr. Raju and the company's global head of internal audit used a number of different techniques to perpetrate the fraud. "Using his personal computer, Mr. Raju created numerous bank statements to advance the fraud. Mr. Raju falsified the bank accounts to inflate the balance sheet with balances that did not exist. He inflated the income statement by claiming interest income from the fake bank accounts. Mr. Raju also revealed that he created 6000 fake salary accounts over the past few years and appropriated the money after the company deposited it. The company's global head of internal audit created fake customer identities and generated fake invoices against their names to inflate revenue. The global head of internal audit also forged board resolutions and illegally obtained loans for the company" [27]. It also appeared that the cash that the company raised through American Depository Receipts in the United States never made it to the balance sheets.

Greed for money, power, competition, success and prestige compelled Mr. Raju to "ride the tiger", which led to violation of all duties imposed on them as fiduciaries—the duty of care, the duty of negligence, the duty of loyalty, the duty of disclosure towards the stakeholders. "The Satyam scandal is a classic case of negligence of fiduciary duties, total collapse of ethical standards, and a lack of corporate social responsibility. It is human greed and desire that led to fraud. This type of behavior can be traced to: greed overshadowing the responsibility to meet fiduciary duties; fierce competition and the need to im- press stakeholders especially investors, analysts, share- holders, and the stock market; low ethical and moral standards by top management; and, greater emphasis on short-term performance" [28]. According to CBI, the In- dian crime investigation agency, the fraud activity dates back from April 1999, when the company embarked on a road to double-digit annual growth. As of December 2008, Satyam had a total market capitalization of $3.2 billion dollars.

Satyam planned to acquire a 51% stake in Maytas In- frastructure Limited, a leading infrastructure develop- ment, construction and project management company, for

$300 million. Here, the Rajus's had a 37% stake. The total turnover was $350 million and a net profit of $20 million. Raju's also had a 35% share in Maytas Proper- ties, another real-estate investment firm. Satyam reve- nues exceeded $1 billion in 2006. In April, 2008 Satyam became the first Indian company to publish IFRS audited financials. On December 16, 2008, the Satyam board, including its five independent directors had approved the founder's proposal to buy the stake in Maytas Infrastruc- ture and all of Maytas Properties, which were owned by family members of Satyam's Chairman, Ramalinga Raju, as fully owned subsidiary for $1.6 billion. Without shareholder approval, the directors went ahead with the management's decision. The decision of acquisition was, however, reversed twelve hours after investors sold Sat- yam's stock and threatened action against the manage- ment. This was followed by the law-suits filed in the US contesting Maytas deal. The World Bank banned Satyam from conducting business for 8 years due to inappropri- ate payments to staff and inability to provide information sought on invoices. Four independent directors quit the Satyam board and SEBI ordered promoters to disclose pledged shares to stock exchange.

Investment bank DSP Merrill Lynch, which was ap- pointed by Satyam to look for a partner or buyer for the company, ultimately blew the whistle and terminated its engagement with the company soon after it found finan- cial irregularities [29]. On 7 January 2009, Saytam's Chairman, Ramalinga Raju, resigned after notifying board members and the Securities and Exchange Board of India (SEBI) that Satyam's accounts had been falsified. Raju confessed that Satyam's balance sheet of September 30, 2008, contained the following irregularies: "He faked figures to the extent of Rs. 5040 crore of non-existent cash and bank balances as against Rs. 5361 crore in the books, accrued interest of Rs. 376 crore (non-existent), understated liability of Rs. 1230 crore on account of funds raised by Raju, and an overstated debtor's position of Rs. 490 crore. He accepted that Satyam had reported revenue of Rs. 2700 crore and an operating margin of Rs. 649 crore, while the actual revenue was Rs. 2112 crore and the margin was Rs. 61 crore". In other words, Raju: 1) inflated figures for cash and bank balances of US $1.04 billion vs. US $1.1 billion reflected in the books; 2) an accrued interest of US $77.46 million which was non-

existent; 3) an understated liability of US $253.38 mil- lion on account of funds was arranged by himself; and 4) an overstated debtors' position of US $100.94 million vs. US $546.11 million in the books.

Raju claimed in the same letter that “neither he nor the managing director had benefited financially from the inflated revenues, and none of the board members had any knowledge of the situation in which the company was placed”. The fraud took place to divert company funds into real-estate investment, keep high earnings per share, raise executive compensation, and make huge profits by selling stake at inflated price. The gap in the balance sheet had arisen purely on account of inflated profits over a period that lasted several years starting in April 1999. “What accounted as a marginal gap between actual operating profit and the one reflected in the books of accounts continued to grow over the years. This gap reached unmanageable proportions as company opera- tions grew significantly”, Ragu explained in his letter to the board and shareholders. He went on to explain, “Every attempt to eliminate the gap failed, and the aborted Maytas acquisition deal was the last attempt to fill the fictitious assets with real ones. But the investors thought it was a brazen attempt to siphon cash out of Satyam, in which the Raju family held a small stake, into firms the family held tightly”. **Table 1** depicts some parts of the Satyam’s fabricated ‘Balance Sheet and Income Statement’ and shows the “difference” between “actual” and “reported” finances.

Fortunately, the Satyam deal with Matyas was “sal- vageable”. It could have been saved only if “the deal had been allowed to go through, as Satyam would have been able to use Maytas’ assets to shore up its own books”. Raju, who showed “artificial” cash on his books, had planned to use this “non-existent” cash to acquire the two Maytas companies. As part of their “tunneling” strategy, the Satyam promoters had substantially reduced their holdings in company from 25.6% in March 2001 to 8.74% in March 2008. Furthermore, as the promoters held a very small percentage of equity (mere 2.18%) on December 2008, as shown in **Table 2**, the concern was that poor performance would result in a takeover bid, thereby exposing the gap. It was like “riding a tiger, not knowing how to get off without being eaten”. The aborted Maytas acquisition deal was the final, desperate effort to cover up the accounting fraud by bringing some real assets into the business. When that failed, Raju con- fessed the fraud. Given the stake the Rajus held in Mat- yas, pursuing the deal would not have been terribly dif- ficult from the perspective of the Raju family. Unlike Enron, which sank due to agency problem, Satyam was brought to its knee due to tunneling. The company with a huge cash pile, with promoters still controlling it with a small per cent of shares (less than 3%), and trying to ab- sorb a real-estate company in which they have a majority stake is a deadly combination pointing prima facie to tunneling [30]. The reason why Ramalinga Raju claims that he did it was because every year he was fudging revenue figures and since expenditure figures could not be fudged so easily, the gap between “actual” profit and “book” profit got widened every year. In order to close this gap, he had to buy Maytas Infrastructure and Maytas

Properties. In this way, "fictitious" profits could be ab- sorbed through a "self-dealing" process. The auditors, bankers, and SEBI, the market watchdog, were all blamed for their role in the accounting fraud.

Table 1. Fabricated balance sheet and income statement of Satyam: as of September 30, 2008. Items Rs. in crore	**Actual**	**Reported**	**Difference**
Cash and Bank Balances	321	5361	5040
Accrued Interest on Bank Fixed Deposits	Nil	376.5	376
Understated Liability	1230	None	1230
Overstated Debtors	2161	2651	490
Total	Nil	Nil	7136
Revenues (Q2 FY 2009)	2112	2700	588
Operating Profits	61	649	588

4.3. The Auditors Role and Factors Contributing to Fraud

Global auditing firm, PricewaterhouseCoopers (PwC), audited Satyam's books from June 2000 until the discov- ery of the fraud in 2009. Several commentators criticized PwC harshly for failing to detect the fraud. Indeed, PwC signed Satyam's financial statements and was responsible for the numbers under the Indian law. One particularly

troubling item concerned the $1.04 billion that Satyam claimed to have on its balance sheet in "non-interest- bearing" deposits. According to accounting professionals, "any reasonable company would have either invested the money into an interest-bearing account, or returned the excess cash to the shareholders. The large amount of cash thus should have been a 'red-flag' for the auditors that further verification and testing was necessary. Further- more, it appears that the auditors did not independently verify with the banks in which Satyam claimed to have deposits". Additionally, the Satyam fraud went on for a number of years and involved both the manipulation of balance sheets and income statements. Whenever Satyam needed more income to meet analyst estimates, it simply created "fictitious" sources and it did so numerous times, without the auditors ever discovering the fraud. Suspiciously, Satyam also paid PwC twice what other firms would charge for the audit, which raises questions about whether PwC was complicit in the fraud. Furthermore, PwC au- dited the company for nearly 9 years and did not uncover the fraud, whereas Merrill Lynch discovered the fraud as part of its due diligence in merely 10 days. Missing these "red-flags" implied either that the auditors were grossly inept or in collusion with the company in committing the fraud. PWC initially asserted that it performed all of the company's audits in accordance with applicable auditing standards.

Numerous factored contributed to the Satyam fraud. The independent board members of Satyam, the institu- tional investor community, the SEBI, retail investors, and the external auditor—none of them, including profes- sional

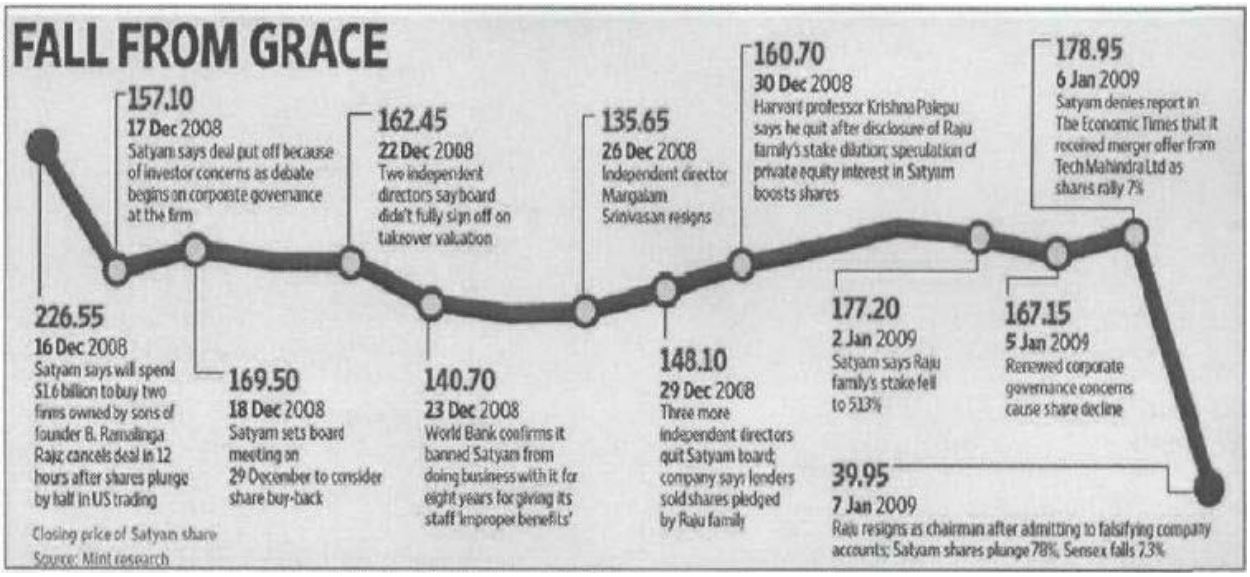
investors with detailed information and models available to them, detected the malfeasance. The follow- ing is a list of factors that contributed to the fraud: greed, ambitious corporate growth, deceptive reporting prac- tices—lack of transparency, excessive interest in main- taining stock prices, executive incentives, stock market expectations, nature of accounting rules, ESOPs issued to those who prepared fake bills, high risk deals that went sour, audit failures (internal and external), aggressiveness of investment and commercial banks, rating agencies and investors, weak independent directors and audit commit- tee, and whistle-blower policy not being effective.

4.4. Aftermath of Satyam Scandal

Immediately following the news of the fraud, Merrill Lynch terminated its engagement with Satyam, Credit Suisse suspended its coverage of Satyam, and Pricewa- terhouseCoopers (PwC) came under intense scrutiny and its license to operate was revoked. Coveted awards won by Satyam and its executive management were stripped from the company. Satyam's shares fell to 11.50 rupees on January 10, 2009, their lowest level since March 1998, compared to a high of 544 rupees in 2008. In the New York Stock Exchange, Satyam shares peaked in 2008 at US $ 29.10; by March 2009 they were trading around US $1.80. Thus, investors lost $2.82 billion in Satyam. Un- fortunately, Satyam significantly inflated its earnings and assets for years and rolling down Indian stock markets and throwing the industry into turmoil [31]. Criminal charges were brought against Mr. Raju, including: criminal conspiracy, breach of trust, and forgery. After the Satyam fiasco and the role played by PwC, investors became wary of those companies who are clients of PwC, which resulted in fall in share prices of around 100 com- panies varying between 5% - 15%. The news of the scandal (quickly compared with the collapse of Enron) sent jitters through the Indian stock market, and the benchmark Sensex index fell more than 5%. Shares in Satyam fell more than 70%. The chart titled as "Fall from grace", shown in **Exhibit 1** depicts the Satyam's stock decline between December 2008 and January 2009.

Immediately after Raju's revelation about the ac- counting fraud, "new" board members were appointed and they started working towards a solution that would prevent the total collapse of the firm. Indian officials acted quickly to try to save Satyam from the same fate that met Enron and WorldCom, when they experienced large accounting scandals. The Indian government "im- mediately started an investigation, while at the same time limiting its direct participation, with Satyam because it did not want to appear like it was responsible for the fraud, or attempting to cover up the fraud". The govern- ment appointed a "new" board of

directors for Satyam to try to save the company. The Board's goal was "to sell the company within 100 days". To devise a plan of sale, the board met with bankers, accountants, lawyers, and gov- ernment officials immediately. It worked diligently to bring stability and confidence back to the company to ensure the sale of the company within the 100-day time frame. To accomplish the sale, the board hired Goldman Sachs and Avendus Capital and charged them with selling the company in the shortest time possible.



By mid-March, several major players in the IT field had gained enough confidence in Satyam's operations to par- ticipate in an auction process for Satyam. The Securities and Exchange Board of India (SEBI) appointed a retired Supreme Court Justice, Justice Bharucha, to oversee the process and instill confidence in the transaction. Several companies bid on Satyam on April 13, 2009. The winning bidder, Tech Mahindra, bought Satyam for $1.13 per share—less than a third of its stock market value before Mr. Raju revealed the fraud—and salvaged its operations [32]. Both Tech Mahindra and the SEBI are now fully aware of the full extent of the fraud and India will not pursue further investigations. The stock has again stabi- lized from its fall on November 26, 2009 and, as part of Tech Mahindra, Saytam is once again on its way toward a bright future.

4.5. Investigation: Criminal and Civil Charges

The investigation that followed the revelation of the fraud has led to charges against several different groups of people involved with Satyam. Indian authorities arrested Mr. Raju, Mr. Raju's brother, B. Ramu Raju, its former managing director, Srinivas Vdlamani, the company's head of internal audit, and its CFO on criminal charges of fraud. Indian authorities also arrested and charged

several of the company's auditors (PwC) with fraud. The Institute of Chartered Accountants of India [33] ruled that "the CFO and the auditor were guilty of professional miscon- duct". The CBI is also in the course of investigating the CEO's overseas assets. There were also several civil charges filed in the US against Satyam by the holders of its ADRs. The investigation also implicated several Indian politicians. Both civil and criminal litigation cases con- tinue in India and civil litigation continues in the United States. Some of the main victims were: employees, clients, shareholders, bankers and Indian government.

In the aftermath of Satyam, India's markets recovered and Satyam now lives on. India's stock market is currently trading near record highs, as it appears that a global eco- nomic recovery is taking place. Civil litigation and criminal charges continue against Satyam. Tech Mahindra purchased 51% of Satyam on April 16, 2009, successfully saving the firm from a complete collapse. With the right changes, India can minimize the rate and size of ac- counting fraud in the Indian capital markets.

4.6. Corporate Governance Issues at Satyam

On a quarterly basis, Satyam earnings grew. Mr. Raju admitted that the fraud which he committed amounted to nearly $276 million. In the process, Satyam grossly vio- lated all rules of corporate governance [34]. The Satyam scam had been the example for following "poor" CG practices. It had failed to show good relation with the shareholders and employees. CG issue at Satyam arose because of non-fulfillment of obligation of the company towards the various stakeholders. Of specific interest are the following: distinguishing the roles of board and management; separation of the roles of the CEO and chairman; appointment to the board; directors and execu- tive compensation; protection of shareholders rights and their executives.

4.7. Lessons Learned from Satyam Scam

The 2009 Satyam scandal in India highlighted the ne- farious potential of an improperly governed corporate leader. As the fallout continues, and the effects were felt throughout the global economy, the prevailing hope is that some good can come from the scandal in terms of lessons learned [35]. Here are some lessons learned from the Satyam Scandal:

Investigate All Inaccuracies: The fraud scheme at Satyam started very small, eventually growing into $276 million white-elephant in the room. Indeed, a lot of fraud schemes initially start out small, with the perpetrator thinking that small changes here and there would not make a big difference, and is less likely to be detected. This sends a message to a lot of com- panies: if your accounts are not balancing, or if something seems inaccurate (even just a tiny bit), it is worth investigating. Dividing responsibilities across a team of people makes it easier to detect irregularities or misappropriated funds.

Ruined Reputations: Fraud does not just look bad on a company; it looks bad on the whole industry and a country. “India’s biggest corporate scandal in memory threatens future foreign investment flows into Asia’s third largest economy and casts a cloud over growth in its once-booming outsourcing sector. The news sent Indian equity markets into a tail-spin, with Bombay’s main benchmark index tumbling 7.3% and the Indian rupee fell”. Now, because of the Satyam scandal, Indian rivals will come under greater scrutiny by the regulators, investors and customers.

Corporate Governance Needs to Be Stronger: The Satyam case is just another example supporting the need for stronger CG. All public-companies must be careful when selecting executives and top-level managers. These are the people who set the tone for the company: if there is corruption at the top, it is bound to trickle-down. Also, separate the role of CEO and Chairman of the Board. Splitting up the roles, thus, helps avoid situations like the one at Satyam.

The Satyam Computer Services’ scandal brought to light the importance of ethics and its relevance to corpo- rate culture. The fraud committed by the founders of Satyam is a testament to the fact that “the science of conduct” is swayed in large by human greed, ambition, and hunger for power, money, fame and glory.

5. Conclusions

Recent corporate frauds and the outcry for transparency and honesty in reporting have given rise to two outcomes. First, forensic accounting skills have become very crucial in untangling the complicated accounting maneuvers that have obfuscated financial statements. Second, public demand for change and subsequent regulatory action has transformed CG scenario across the globe. In fact, both these trends have the common goal of addressing the investors’ concerns about the transparent financial re- porting system. The failure of the corporate communica- tion structure, therefore, has made the financial community realize that “there is a great need for skilled profes- sionals that can identify, expose, and prevent structural weaknesses in three key areas: poor corporate govern- ance, flawed internal controls, and fraudulent financial statements [36]. In addition, the CG framework needs to be first of all strengthened and then implemented in “let- ter as well as in right spirit”. The increasing rate of white-collar crimes, without doubt, demands stiff penal- ties and punishments.

Perhaps, no financial fraud had a greater impact on accounting and auditing profession than Enron, World- Com, and recently, India’s Enron: “Satyam”. All these frauds have led to the passage of the Sarbanes-Oxley Act in July 2002, and a new federal agency and financial standard-setting body, the Public Companies Accounting Oversight Board (PCAOB). It also was the impetus for the American

Institute of Certified Public Accountants' (AICPA) adoption of SAS No. 99, "Consideration of Fraud in a Financial Statement Audit" [37]. But it may be that the greatest impact of Enron and WorldCom was in the significant increased focus and awareness related to fraud. It establishes external auditors' responsibility to plan and perform audits to provide a reasonable assur- ance that the audited financial statements are free of ma- terial frauds.

As part of this research study, one of the key objectives was "to examine and analyze in-depth the Satyam Com- puters Limited's accounting scandal by portraying the sequence of events, the aftermath of events, the key par- ties involved, major reforms undertaken in India, and learn some lessons from it". Unlike Enron, which sank due to "agency" problem, Satyam was brought to its knee due to "tunneling". The Satyam scandal highlights the importance of securities laws and CG in emerging mar- kets. There is a broad consensus that emerging market countries must strive to create a regulatory environment in their securities markets that fosters effective CG. India has managed its transition into a global economy well, and although it suffers from CG issues, it is not alone as both developed countries and emerging countries ex- perience accounting and CG scandals. The Satyam scan- dal brought to light, once again, the importance of ethics and its relevance to corporate culture. The fraud com- mitted by the founders of Satyam is a testament to the fact that "the science of conduct is swayed in large by human greed, ambition, and hunger for power, money, fame and glory". All kind of scandals/frauds have proven that there is a need for good conduct based on strong ethics. The Indian government, in Satyam case, took very quick actions to protect the interest of the investors, safeguard the credibility of India, and the nation's image across the world. Moreover, Satyam fraud has forced the government to re-write CG rules and tightened the norms for auditors and accountants. The Indian affiliate of PwC "routinely failed to follow the most basic audit proce- dures. The SEC and the PCAOB fined the affiliate, PwC India, $7.5 million which was described as the largest American penalty ever against a foreign accounting firm" [38]. According to President, ICAI (January 25, 2011), "The Satyam scam was not an accounting or auditing failure, but one of CG. This apex body had found the two PWC auditors prima-facie guilty of professional mis- conduct". The CBI, which investigated the Satyam fraud case, also charged the two auditors with "complicity in the commission of the fraud by consciously overlooking the accounting irregularities".

The culture at Satyam, especially dominated by the board, symbolized an unethical culture. On one hand, his rise to stardom in the corporate world, coupled with im- mense pressure to impress investors, made Mr. Raju a "compelled leader to deliver outstanding results". On the contrary, Mr. Raju had to suppress his own morals and values in favor of the greater good of the company. The board connived with his actions and stood as a blind spectator; the lure of big compensation to members fur- ther encouraged such behavior. But, in the end, truth is sought and those violating the legal, ethical, and societal norms are taken

to task as per process of law. The public confession of fraud by Mr. Ramalinga Raju speaks of integrity still left in him as an individual. His acceptance of guilt and blame for the whole fiasco shows a bright

spot of an otherwise “tampered” character. After quitting as Satyam’s Chairman, Raju said, “I am now prepared to subject myself to the laws of land and face consequences thereof”. Mr. Raju had many ethical dilemmas to face, but his persistent immoral reasoning brought his own demise. The fraud finally had to end and the implications were having far reaching consequences. Thus, Satyam scam was not an accounting or auditing failure, but one of CG. Undoubtedly, the government of India took prompt actions to protect the interest of the investors and safeguard the credibility of India and the nation’s image across the world. In addition, the CG framework needs to be strengthened, implemented both in “letter as well as in right spirit”, and enforced vigorously to curb white-collar crimes.

HARSHAD MEHTA CASE

Ketan parekh case

UNIT TRUST OF INDIA CASE

The 10 Worst Corporate Accounting Scandals of All Time

If there is one theme to rival terrorism for defining the last decade-and-a-half, it would have to be corporate greed and malfeasance. Many of the biggest corporate accounting scandals in history happened during that time. Here's a chronological look back at some of the worst examples.

Waste Management Scandal (1998)

- Company: Houston-based publicly traded waste management company
- What happened: Reported $1.7 billion in fake earnings.
- Main players: Founder/CEO/Chairman Dean L. Buntrock and other top executives; Arthur Andersen Company (auditors)
- How they did it: The company allegedly falsely increased the depreciation time length for their property, plant and equipment on the balance sheets.
- How they got caught: A new CEO and management team went through the books.
- Penalties: Settled a shareholder class-action suit for $457 million. SEC fined ArthurAndersen $7 million.
- Fun fact: After the scandal, new CEO A. Maurice Meyers set up an anonymous company hotline where employees could report dishonest or improper behavior.

Enron Scandal (2001)

- Company: Houston-based commodities, energy and service corporation
- What happened: Shareholders lost $74 billion, thousands of employees and investors lost their retirement accounts, and many employees lost their jobs.
- Main players: CEO Jeff Skilling and former CEO Ken Lay.
- How they did it: Kept huge debts off balance sheets.
- How they got caught: Turned in by internal whistleblower Sherron Watkins; high stock prices fueled external suspicions.
- Penalties: Lay died before serving time; Skilling got 24 years in prison. The company filed for bankruptcy. Arthur Andersen was found guilty of fudging Enron's accounts.
- Fun fact: Fortune Magazine named Enron "America's Most Innovative Company" 6 years in a row prior to the scandal.

WorldCom Scandal (2002)

- Company: Telecommunications company; now MCI, Inc.
- What happened: Inflated assets by as much as $11 billion, leading to 30,000 lost jobs and $180 billion in losses for investors.
- Main player: CEO Bernie Ebbers
- How he did it: Underreported line costs by capitalizing rather than expensing and inflated revenues with fake accounting entries.

- How he got caught: WorldCom's internal auditing department uncovered $3.8 billion of fraud.
- Penalties: CFO was fired, controller resigned, and the company filed for bankruptcy. Ebbers sentenced to 25 years for fraud, conspiracy and filing false documents with regulators.
- Fun fact: Within weeks of the scandal, Congress passed the Sarbanes-Oxley Act, introducing the most sweeping set of new business regulations since the 1930s.

Tyco Scandal (2002)

- Company: New Jersey-based blue-chip Swiss security systems.
- What happened: CEO and CFO stole $150 million and inflated company income by $500 million.
- Main players: CEO Dennis Kozlowski and former CFO Mark Swartz.
- How they did it: Siphoned money through unapproved loans and fraudulent stock sales. Money was smuggled out of company disguised as executive bonuses or benefits.
- How they got caught: SEC and Manhattan D.A. investigations uncovered questionable accounting practices, including large loans made to Kozlowski that were then forgiven.
- Penalties: Kozlowski and Swartz were sentenced to 8-25 years in prison. A class-action lawsuit forced Tyco to pay $2.92 billion to investors.
- Fun fact: At the height of the scandal Kozlowski threw a $2 million birthday party for his wife on a Mediterranean island, complete with a Jimmy Buffet performance.

HealthSouth Scandal (2003)

- Company: Largest publicly traded health care company in the U.S.
- What happened: Earnings numbers were allegedly inflated $1.4 billion to meet stockholder expectations.
- Main player: CEO Richard Scrushy.
- How he did it: Allegedly told underlings to make up numbers and transactions from 1996-2003.
- How he got caught: Sold $75 million in stock a day before the company posted a huge loss, triggering SEC suspicions.
- Penalties: Scrushy was acquitted of all 36 counts of accounting fraud, but convicted of bribing the governor of Alabama, leading to a 7-year prison sentence.
- Fun fact: Scrushy now works as a motivational speaker and maintains his innocence.

Freddie Mac (2003)

- Company: Federally backed mortgage-financing giant.
- What happened: $5 billion in earnings were misstated.
- Main players: President/COO David Glenn, Chairman/CEO Leland Brendsel, ex-CFO Vaughn Clarke, former senior VPs Robert Dean and Nazir Dossani.
- How they did it: Intentionally misstated and understated earnings on the books.
- How they got caught: An SEC investigation.
- Penalties: $125 million in fines and the firing of Glenn, Clarke and Brendsel.
- Fun fact: 1 year later, the other federally backed mortgage financing company, Fannie Mae, was caught in an equally stunning accounting scandal.

American International Group (AIG) Scandal (2005)

- Company: Multinational insurance corporation.
- What happened: Massive accounting fraud to the tune of $3.9 billion was alleged, along with bid-rigging and stock price manipulation.
- Main player: CEO Hank Greenberg.
- How he did it: Allegedly booked loans as revenue, steered clients to insurers with whom AIG had payoff agreements, and told traders to inflate AIG stock price.
- How he got caught: SEC regulator investigations, possibly tipped off by a whistleblower.
- Penalties: Settled with the SEC for $10 million in 2003 and $1.64 billion in 2006, with a Louisiana pension fund for $115 million, and with 3 Ohio pension funds for $725 million. Greenberg was fired, but has faced no criminal charges.
- Fun fact: After posting the largest quarterly corporate loss in history in 2008 ($61.7 billion) and getting bailed out with taxpayer dollars, AIG execs rewarded themselves with over $165 million in bonuses.

Lehman Brothers Scandal (2008)

- Company: Global financial services firm.
- What happened: Hid over $50 billion in loans disguised as sales.
- Main players: Lehman executives and the company's auditors, Ernst & Young.
- How they did it: Allegedly sold toxic assets to Cayman Island banks with the understanding that they would be bought back eventually. Created the impression Lehman had $50 billion more cash and $50 billion less in toxic assets than it really did.
- How they got caught: Went bankrupt.

- Penalties: Forced into the largest bankruptcy in U.S. history. SEC didn't prosecute due to lack of evidence.
- Fun fact: In 2007 Lehman Brothers was ranked the #1 "Most Admired Securities Firm" by Fortune Magazine.

Bernie Madoff Scandal (2008)

- Company: Bernard L. Madoff Investment Securities LLC was a Wall Street investment firm founded by Madoff.
- What happened: Tricked investors out of $64.8 billion through the largest Ponzi scheme in history.
- Main players: Bernie Madoff, his accountant, David Friehling, and Frank DiPascalli.
- How they did it: Investors were paid returns out of their own money or that of other investors rather than from profits.
- How they got caught: Madoff told his sons about his scheme and they reported him to the SEC. He was arrested the next day.
- Penalties: 150 years in prison for Madoff + $170 billion restitution. Prison time for Friehling and DiPascalli.
- Fun fact: Madoff's fraud was revealed just months after the 2008 U.S. financial collapse.

Satyam Scandal (2009)

- Company: Indian IT services and back-office accounting firm.
- What happened: Falsely boosted revenue by $1.5 billion.
- Main player: Founder/Chairman Ramalinga Raju.
- How he did it: Falsified revenues, margins and cash balances to the tune of 50 billion rupees.
- How he got caught: Admitted the fraud in a letter to the company's board of directors.
- Penalties: Raju and his brother charged with breach of trust, conspiracy, cheating and falsification of records. Released after the Central Bureau of Investigation failed to file charges on time.
- Fun fact: In 2011 Ramalinga Raju's wife published a book of his existentialist, free-verse poetry.

Thank You.

The Prevention of Money-laundering Act, 2002
1
THE PREVENTION OF MONEY-LAUNDERING
ACT, 2002
INTRODUCTION

Money-laundering poses a serious threat not only to the financial systems of countries, but also to their integrity and sovereignty. To obviate such threats international community has taken some initiatives. It has been felt that to prevent money-laundering and connected activities a comprehensive legislation is urgently needed. To achieve this objective the Prevention of Money-laundering Bill, 1998 was introduced in the Parliament. The Bill was referred to the Standing Committee on Finance, which presented its report on 4th March, 1999 to the Lok Sabha. The Central Government broadly accepted the recommendation of the Standing Committee and incorporated them in the said Bill along with some other desired changes.

STATEMENT OF OBJECTS AND REASONS

It is being realised, world over, that money-laundering poses a serious threat not only to the financial systems of countries, but also to their integrity and sovereignty. Some of the initiatives taken by the international community to obviate such threat are outlined below:—

(a)
the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, to which India is a party, calls for prevention of laundering of proceeds of drug crimes and other connected activities and confiscation of proceeds derived from such offence.

(b)
the Basle Statement of Principles, enunciated in 1989, outlined basic policies and procedures that banks should follow in order to assist the law enforcement agencies in tackling the problem of money-laundering.

(c)
the Financial Action Task Force established at the summit of seven major industrial nations, held in Paris from 14th to 16th July, 1989, to examine the problem of money-laundering has made forty recommendations, which provide the foundation material for comprehensive legislation to combat the problem of money-laundering. The recommendations were classified under various heads. Some of the important heads are—

(i)
declaration of laundering of monies carried through serious crimes a criminal offence;

(ii)
to work out modalities of disclosure by financial institutions regarding reportable transactions;

(iii)
confiscation of the proceeds of crime;

(iv)

declaring money-laundering to be an extraditable offence; and
(v)
promoting international co-operation in investigation of money-laundering.
1
(d)
the Political Declaration and Global Programme of Action adopted by United Nations General Assembly by its Resolution No. S-17/2 of 23rd February, 1990,
inter alia
, calls upon the member States to
develop mechanism to prevent financial institutions from being used for laundering of drug related money and enactment of legislation to prevent such laundering.
(e)
the United Nations in the Special Session on countering World Drug Problem Together concluded on the 8th to the 10th June, 1998 has made another declaration regarding the need to combat money-laundering. India is a signatory to this declaration.
2. In view of an urgent need for the enactment or a comprehensive legislation
inter alia
for preventing money-laundering and connected activities
confiscation of proceeds of crime, setting up of agencies and mechanisms for co-ordinating measures for combating money-laundering, etc., the Prevention of Money-Laundering Bill, 1998 was introduced in the Lok Sabha on the 4th August, 1998. The Bill was referred to the Standing Committee on Finance, which presented its report on the 4th March, 1999 to the Lok Sabha. The recommendations of the Standing Committee accepted by the Central Government are that (a) the expressions “banking company” and “person” may be defined; (b) in Part I of the Schedule under Indian Penal Code the word offence under section 477A relating to falsification of accounts should be omitted; (c) ‘knowingly’ be inserted in clause 3(b) relating to the definition of money-laundering; (d) the banking companies financial institutions and intermediaries should be required to furnish information of transactions to the Director instead of Commissioner of Income-tax (e) the banking companies should also be brought within the ambit of clause II relating to obligations of financial institutions and intermediaries; (f) a definite time-limit of 24 hours should be provided for producing a person about to be searched or arrested person before the Gazetted Officer or Magistrate; (g) the words “unless otherwise proved to the satisfaction of the authority concerned” may be inserted in clause 22 relating to presumption on inter-connected transactions; (h) vacancy in the office of the Chairperson of an Appellate Tribunal, by reason of his death, resignation or

otherwise, the senior-most member shall act as the Chairperson till the date on which a new Chairperson appointed in accordance with the provisions of this Act to fill the vacancy, enters upon his office; (i) the appellant before the Appellate Tribunal may be authorised to engage any authorised representative as defined under section 288 of the Income-tax Act, 1961, (j) the punishment for vexatious search and for false information may be enhanced from three months imprisonment to two years imprisonment, or fine of rupees ten thousand to fine of rupees fifty thousand or both; (k) the word 'good faith' may be incorporated in the clause relating to Bar of legal proceedings. The Central Government have broadly accepted the above recommendations and made provisions of the said recommendations in the Bill.

3. In addition to above recommendations of the standing committee the Central Government proposes to (a) relax the conditions prescribed for grant of bail so that the Court may grant bail to a person who is below sixteen years of age, or woman, or sick or infirm, (b) levy of fine for default of non-compliance of the issue of summons, etc. (c) make provisions for having reciprocal

arrangement for assistance in certain matters and procedure for attachment and confiscation of property so as to facilitate the transfer of funds involved in money-laundering kept outside the country and extradition of the accused persons from abroad.

4. The Bill seeks to achieve the above objects.

ACT 15 OF 2003

The Prevention of Money-Laundering Bill having been passed by both the Houses of Parliament received the assent of the President on 17th January, 2003. It came on the Statute Book as THE PREVENTION OF MONEY-LAUNDERING ACT, 2002 (15 of 2003).

LIST OF AMENDING ACTS

1. The Prevention of Money-Laundering (Amendment) Act, 2005 (20 of 2005) (w.e.f. 1-7-2005).
2. The Prevention of Money-Laundering (Amendment) Act, 2009 (21 of 2009) (w.e.f. 1-6-2009).
3. The Prevention of Money-Laundering (Amendment) Act, 2012 (2 of 2013) (w.e.f. 15-2-2013).

4
1.
Came into force on 1-7-2005,
vide
G.S.R. 436(E), dated 1st July, 2005, published in the Gazette
of India, Extra., Pt. II, Sec. 3(i), dated 1st July, 2005.
THE PREVENTION OF MONEY
-LAUNDERING
ACT, 2002
(15
of
2003)
[
17th January, 2003
]
An Act to prevent money-laundering and to provide for confiscation of property derived from, or involved in, money-laundering and for matters connected therewith or
incidental thereto.
W
HEREAS
the Political Declaration and Global Programme of Action, annexed
to the resolution S-17/2 was adopted by the General Assembly of the United Nations at its seventeenth special session on the twenty-third day of February, 1990;
A
ND
WHEREAS
the Political Declaration adopted by the Special Session of the
United Nations General Assembly held on 8th to 10th June, 1998 calls upon the Member States to adopt national money-laundering legislation and programme;
A
ND
WHEREAS
it is considered necessary to implement the aforesaid resolution
and the Declaration;
B
E
it enacted by Parliament in the Fifty-third Year of the Republic of India
as follows:—
CHAPTER I
PRELIMINARY
1. Short title, extent and commencement.

—(1) This Act may be called the
Prevention of Money-laundering Act, 2002.
(2) It extends to the whole of India.
(3) It shall come into force on such date
1
as the Central Government may, by
notification in the Official Gazette, appoint, and different dates may be
appointed for different provisions of this Act and any reference in any such
provision to the commencement of this Act shall be construed as a reference to
the coming into force of that provision.
2. Definitions.
—(1) In this Act, unless the context otherwise requires,—
(a)
"Adjudicating Authority" means an Adjudicating Authority
appointed under sub-section (1) of section 6;
(b)
"Appellate Tribunal" means the Appellate Tribunal established
under section 25;
(c)
"Assistant Director" means an Assistant Director appointed under
sub-section (1) of section 49;
(d)
"attachment" means prohibition of transfer, conversion, disposition
or movement of property by an order issued under Chapter III;
The Prevention of Money-laundering Act, 2002
5
1
[(da)
"authorised person" means an authorised person as defined in
clause (c) of section 2 of the Foreign Exchange Management Act, 1999
(42 of 1999);]
(e)
"banking company" means a banking company or a co-operative
bank to which the Banking Regulation Act, 1949 (10 of 1949) applies
and includes any bank or banking institution referred to in section 51
of that Act;
(f)
"Bench" means a Bench of the Appellate Tribunal;
2
[(fa)
"beneficial owner" means an individual who ultimately owns or
controls a client of a reporting entity or the person on whose behalf
a transaction is being conducted and includes a person who exercises

ultimate effective control over a juridical person;]
(g)
“Chairperson” means the Chairperson of the Appellate Tribunal;
(h)
“chit fund company” means a company managing, conducting or supervising, as foreman, agent or in any other capacity, chits as defined in section 2 of the Chit Funds Act, 1982 (40 of 1982);
3
[(ha)
“client” means a person who is engaged in a financial transaction or activity with a reporting entity and includes a person on whose behalf the person who engaged in the transaction or activity, is acting;]
(i)
“co-operative bank” shall have the same meaning as assinged to it in clause (dd) of section 2 of the Deposit Insurance and Credit Guarantee Corporation Act, 1961 (47 of 1961);
4
[(ia)
“corresponding law” means any law of any foreign country corresponding to any of the provisions of this Act or dealing with offences in that country corresponding to any of the scheduled offences;]
4
[(ib)
“dealer” has the same meaning as assigned to it in clause (b) of section 2 of the Central Sales Tax Act, 1956 (74 of 1956);]
(j)
“Deputy Director” means a Deputy Director appointed under sub-section (1) of section 49;
5
[***]
(k)
“Director” or “Additional Director” or “Joint Director” means a Director or Additional Director or Joint Director, as the case may be, appointed under sub-section (1) of section 49;
1.
Ins. by Act 21 of 2009, sec. 2(i) (w.e.f. 1-6-2009).
2.
Ins. by Act 2 of 2013, sec. 2(i) (w.e.f. 15-2-2013,
vide
S.O. 343(E), dated 8-2-2013).
3.

Ins. by Act 2 of 2013, sec. 2(ii) (w.e.f. 15-2-2013,
vide
S.O. 343(E), dated 8-2-2013).
4.
Ins. by Act 2 of 2013, sec. 2(iii) (w.e.f. 15-2-2013,
vide
S.O. 343(E), dated 8-2-2013).
5.
Clause (ja) omitted by Act 2 of 2013, sec. 2(iv) (w.e.f. 15-2-2013,
vide
S.O. 343(E), dated
8-2-2013). Earlier clause (ja) was inserted by Act 21 of 2009, sec. 2(ii) (w.e.f. 1-6-2009). Clause
(ja), before omission, stood as under:
‘(ja) “designated business or profession” means carrying on activities for playing games
of chance for cash or kind, and includes such activities associated with casino or such other
activities as the Central Government may, by notification, so designate, from time to time.’.
Sec. 2]
6
The Prevention of Money-laundering Act, 2002
1
[(l)
“financial institution” means a financial institution as defined in clause (c) of section 45-I of the Reserve Bank of India Act, 1934 (2 of 1934) and includes a chit fund company, a housing finance institution, an authorised person, a payment system operator, a non-banking financial company and the Department of Posts in the Government of India;]
(m)
“housing finance institution” shall have the meaning as assigned to it in clause (d) of section 2 of the National Housing Bank Act, 1987 (53 of 1987);
2
[(n)
“intermediary” means,—
(i)
a stock-broker, sub-broker share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser or any other intermediary associated with securities market and

registered under section 12 of the Securities and Exchange Board of India Act, 1992 (15 of 1992); or
(ii)
an association recognised or registered under the Forward Contracts (Regulation) Act, 1952 (74 of 1952) or any member of such association; or
(iii)
intermediary registered by the Pension Fund Regulatory and Development Authority; or
(iv)
a recognised stock exchange referred to in clause (f) of section 2 of the Securities Contracts (Regulation) Act, 1956 (42 of 1956);]
3
[(na)
"investigation" includes all the proceedings under this Act conducted by the Director or by an authority authorised by the Central Government under this Act for the collection of evidence;]
(o)
"Member" means a Member of the Appellate Tribunal and includes the Chairperson;
(p)
"money-laundering" has the meaning assigned to it in section 3;
(q)
"non-banking financial company" shall have the same meaning as assigned to it in clause (f) of section 45-I of the Reserve Bank of India Act, 1934 (2 of 1934)
4
[***];
[Sec. 2
1.
Subs. by Act 2 of 2013, sec. 2(v), for clause (l) (w.e.f. 15-2-2013, vide
S.O. 343(E), dated 8-2-2013).
Earlier clause (l) was amended by Act 21 of 2009, sec. 2(iii) (w.e.f. 1-6-2009). Clause (l), before
substitution, stood as under:
'(l) "financial institution" means a financial institution as defined in clause (c) of section
45-I of the Reserve Bank of India Act, 1934 (2 of 1934) and includes a chit fund company,
a co-operative bank, a housing finance institution and an authorised person, a payment
system operator and a non-banking financial company;'.

2.
Subs. by Act 2 of 2013, sec. 2(vi), for clause (n) (w.e.f. 15-2-2013,
vide
S.O. 343(E), dated
8-2-2013) Clause (n), before substitution, stood as under:
‘(n) “intermediary” means a stock-broker, sub-broker, share transfer agent, banker to an
issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio
manager, investment adviser and any other intermediary associated with securities market
and registered under section 12 of the Securities and Exchange Board of India Act, 1992 (15
of 1992);’.
3.
Ins. by Act 20 of 2005, sec. 2 (w.e.f. 1-7-2005).
4.
The words “and includes a person carrying on designated business or profession”omitted by
Act 2 of 2013, sec. 2(vii) (w.e.f. 15-2-2013,
vide
S.O. 343(E), dated 8-2-2013). Earlier these words
were inserted by Act 21 of 2009, sec. 2(iv) (w.e.f. 1-6-2009).
The Prevention of Money-laundering Act, 2002
7
(r)
“notification” means a notification published in the Official Gazette;
1
[(ra)
“offence of cross border implications”, means—
(i)
any conduct by a person at a place outside India which
constitutes an offence at that place and which would have
constituted an offence specified in Part A, Part B or Part C of the
Schedule, had it been committed in India and if such person
2
[transfers in any manner] the proceeds of such conduct or part
thereof to India; or
(ii)
any offence specified in Part A, Part B or Part C of the Schedule
which has been committed in India and the proceeds of crime, or
part thereof have been transferred to a place outside India or any
attempt has been made to transfer the proceeds of crime, or part

thereof from India to a place outside India.
Explanation
.—Nothing contained in this clause shall adversely
affect any investigation, enquiry, trial or proceeding before any
authority in respect of the offences specified in Part A or Part B of the
Schedule to the Act before the commencement of the Prevention of
Money-laundering (Amendment) Act, 2009.]
1
[(rb)
"payment system" means a system that enables payment to be
effected between a payer and a beneficiary, involving clearing,
payment or settlement service or all of them.
Explanation
.—For the purposes of this clause, "payment system"
includes the systems enabling credit card operations, debit card
operations, smart card operations, money transfer operations or
similar operations;]
1
[(rc)
"payment system operator" means a person who operates a payment
system and such person includes his overseas principal.
Explanation
.—For the purposes of this clause, "overseas principal"
means,—
(A)
in the case of a person, being an individual, such individual
residing outside India, who owns or controls or manages,
directly or indirectly, the activities or functions of payment
system in India;
(B)
in the case of a Hindu undivided family, Karta of such Hindu
undivided family residing outside India who owns or
controls or manages, directly or indirectly, the activities or
functions of payment system in India;
(C)
in the case of a company, a firm, an association of persons, a
body of individuals, an artificial juridical person, whether
incorporated or not, such company, firm, association of
persons, body of individuals, artificial juridical person
incorporated or registered outside India or existing as such
Sec. 2]
1.
Ins. by Act 21 of 2009, sec. 2(v) (w.e.f. 1-6-2009).

2.
Subs. by Act 2 of 2013, sec. 2(viii), for “remits” (w.e.f. 15-2-2013, vide
S.O. 343(E), dated
8-2-2013).

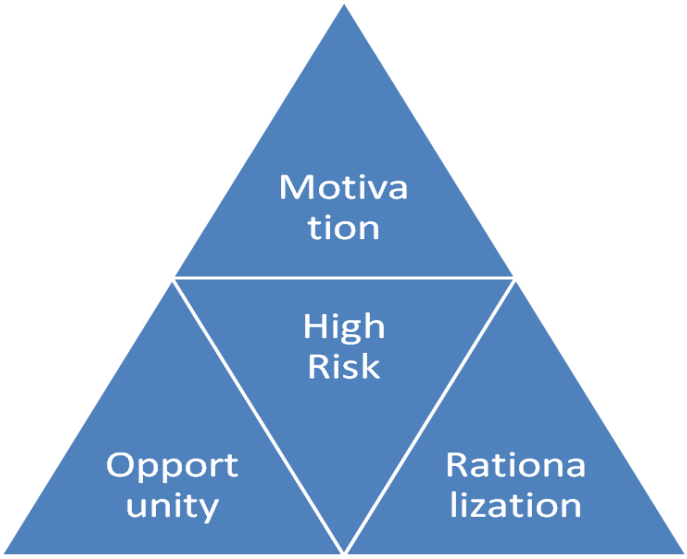
and which owns or controls or manages, directly or indirectly, the activities or functions of payment system in India;]
(s)
“person” includes;—
(i)
an individual,
(ii)
a Hindu undivided family,
(iii)
a company,
(iv)
a firm,
(v)
an association of persons or a body of individuals, whether incorporated or not,
(vi)
every artificial juridical person, not falling within any of the preceding sub-clauses, and
(vii)
any agency, office or branch owned or controlled by any of the above persons mentioned in the preceding sub-clauses;
1
[(sa)
“person carrying on designated business or profession” means,—
(i)
a person carrying on activities for playing games of chance for cash or kind, and includes such activities associated with casino;
(ii)
a Registrar or Sub-Registrar appointed under section 6 of the Registration Act, 1908 (16 of 1908) as may be notified by the Central Government;
(iii)
real estate agent, as may be notified by the Central Government;
(iv)
dealer in precious metals, precious stones and other high value

goods, as may be notified by the Central Government;
(v)
person engaged in safekeeping and administration of cash and liquid securities on behalf of other persons, as may be notified by the Central Government; or
(vi)
person carrying on such other activities as the Central Government may, by notification, so designate, from time-to-time;]
1
[(sb)
"precious metal" means gold, silver, platinum, palladium or rhodium or such other metal as may be notified by the Central Government;]
1
[(sc)
"precious stone" means diamond, emerald, ruby, sapphire or any such other stone as may be notified by the Central Government;]
(t)
"prescribed" means prescribed by rules made under this Act;
(u)
"proceeds of crime" means any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a scheduled offence or the value of any such property;
(v)
"property" means any property or assets of every description, whether corporeal or incorporeal, movable or immovable, tangible or intangible and includes deeds and instruments evidencing title to, or interest in, such property or assets, wherever located;
[Sec. 2
1.
Ins. by Act 2 of 2013, sec. 2(ix) (w.e.f. 15-2-2013, vide
S.O. 343(E), dated 8-2-2013).
The Prevention of Money-laundering Act, 2002
9
1
[
Explanation
.—For the removal of doubts, it is hereby clarified that the term "property" includes property of any kind used in the commission of an offence under this Act or any of the scheduled offences;]
1

[(va)
“real estate agent” means a real estate agent as defined in clause (88) of section 65 of the Finance Act, 1994;]
(w)
“records” include the records maintained in the form of books or stored in a computer or such other form as may be prescribed;
2
[(wa)
“reporting entity” means a banking company, financial institution, intermediary or a person carrying on a designated business or profession;].
(x)
“Schedule” means the Schedule to this Act;
(y)
“scheduled offence” means—
(i)
the offences specified under Part A of the Schedule; or
3
[(ii)
the offences specified under Part B of the Schedule if the total value involved in such offences is thirty lakh rupees or more; or]
3
[(iii)
the offences specified under Part C of the Schedule;]
(z)
“Special Court” means a Court of Session designated as Special Court under sub-section (1) of section 43;
(za)
“transfer” includes sale, purchase, mortgage, pledge, gift, loan or any other form of transfer of right, title, possession or lien;
(zb)
“value” means the fair market value of any property on the date of its acquisition by any person, or if such date cannot be determined, the date on which such property is possessed by such person.
(2) Any reference, in this Act or the Schedule, to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provisions of the corresponding law, if any, in force in that area.
CHAPTER II
OFFENCE OF MONEY-LAUNDERING
3. Offence of money-laundering.
—Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually

involved in any process or activity connected
4
[proceeds of crime including its
concealment, possession, acquisition or use and projecting or claiming] it as untainted property shall be guilty of offence of money-laundering.

WHO COMMITS FRAUD AND WHY ?



WORKPLACE DEVIANCE MODEL

- Only 10% of employees – totally honest
- 10% employees – totally dishonest
- Connotation is :-
- 80 % of the employees capable of being influenced to be honest or dishonest
- 90% of all employees are capable of fraud and dishonesty
- Above concept devised by ACFE

FRAUDSTERS PROFILE

- Dominant Leaders – Bernie Ebbers (Worldcom) Kenneth Lay (Enron) - both perpetuated frauds that led to corporate collapse
- Flamboyant Entrepreneurs – Harshad Mehta, Ramalinga Raju – turned to fraud to sustain illusion of success
- Charismatic People – Bernard Madoff , Allen Stanford, Charles Ponzi , Sahara created organizations for perpetrating fraud

- Rogue Employees – Nick Leeson (Barings) Jerome Kerviel(Societe Generale) authoritative roll

FRAUD PRONE FINANCIAL SECTORS

- Banks, followed by Insurance/NBFC's and Mutual Fund Companies account for nearly 63% of frauds in financial sector.
- Total amount involved in fraud in 2011-12 is approximately INR 38 billion.
- Other main vulnerable fraud areas are : Real Estate,Transport,Telecom,Technology,Health care,Consumer Goods,Mining.

FRAUDS BY CORPORATES

- Overstatement of assets/debtors
- Understatement of liabilities/creditors
- Inflation of income
- False projection of sales
- Inflation of expenses
- Misrepresentation/misreporting of financial statements
- Diversion of loans for other purposes
- Bribery and corruption
- Asset Mismanagement

BANKS-FRAUD PRONE AREAS

- Lax KYC norms/no spot verification/survey
- Window dressing of appraisals
- Incomplete/misleading verification report
- Inflated valuation report/faulty legal opinion
- Forged/false documents for loans
- Transgressing/misuse of financial powers
- Violating terms of sanction/disbursal of funds
- End use of funds not tracked
- Soft on Roll Over/OTS/CDR

GROWING CDR PILE

- March 2009-184 cases-Rs.86,536 cr. debt
- March 2010-215 cases-Rs.1,04,299 cr. Debt
- March 2011-242 cases- Rs.1,10,914 cr. Debt

- March 2012-292 cases-Rs.1,50,515 cr. Debt
- March 2013-401 cases-Rs.2,29,013 cr. Debt
- June 2013-415 cases-Rs.2,50,279 cr. Debt
- Dec.2013-Rs.4,46,300 cr. Debt
- Source: Business Standard/TOI

ONE TIME SETTLEMENTS

- Also known as compromise settlements
- Undue favours by banks to settle claims
- Bank regulations – after OTS drop criminal proceedings
- CBI vs Duncans Agro Industries Ltd. Calcutta(1996) 5 SCC 591
- Nikhil Merchant vs CBI (2008) 9 SCC 677
- CBI vs A. Ravi Shankar Prasad in SLP(crl) 8854-57/2008 in criminal appeal no. 1080-1085 of 2009.

CORRUPTION

- Total bribe paid each year by an adult urban Indian-Rs.6,29,675 crores
- 6.3 % of GDP
- 2,151% more than health expenditure
- 942 % more than education expenditure
- 353% more than defence budget
- 320% more than IT revenue

CASE STUDIES

- Securities Scam-1992
- Collapse of a Bank
- Fraud by a Company
- Initial Public Offer Scam-2006
- Merchanting Trade Transactions

SECURITIES SCAM - 1992

- CRR, SLR Ratios about 63.5%
- Nationalized banks had several social obligations that were loss making.
- With desire for profits tendency to CIRCUMVENT rules crept in.
- PSUs encouraged towards self sufficiency. Parked funds with brokers in violation of laid down norms.

Facets of the Scam

- Security Transactions
- Siphoning of PSU funds
- Call Money Borrowings
- Portfolio Management Scheme
- Bill Discounting facilities
- Coupon rate hike

Reasons for the Scam

- Systemic failure
- Inadequacies in the settlement system
- Poor corporate governance
- The human factor

COLLAPSE OF A BANK

. CMD and GM quit as employees of a bank

- Floated own bank with Rs.100 crores
- Borrowed heavily from investors / group companies
- Lenders were mostly old clients of the bank
- Out standings of favored clients cleared
- Stipulated waiver of Interest on personal loans
- Huge personal holdings
- Rigging of share prices to increase personal fortune
- Reckless sanctioning of credit facilities to group companies
- Appraisal notes sketchy or prepared after sanction / disbursal of loans
- Collateral securities insufficient, faulty, non-existent, non-enforceable, etc.
- Additional loans, enhanced credit facilities sanctioned / disbursed despite huge outstanding
- Credit facilities sanctioned to defunct sister companies for ever greening of accounts.
- Violation of RBI guidelines on Group Exposures Norms / Capital Market Exposure Norms.
- Approval of Committee of Board (COB) obtained on misrepresentation/ suppression of facts.
- Under provisioning/suppression of NPAs to show profits and declare dividends.

SIPHONING FUNDS-ROGUE COMPANY

- Fraudulent issue of preferential shares in the name of trusts.
- No approval of board / AGM.
- Fraudulently obtained ISIN numbers for fully paid up shares which were not even partially subscribed.
- After D-mat, identity / distinctive numbers of shares lost.
- Rigging of share prices
- Synchronized cross deals
- Funds used for purchasing shares of own company by OCB's
- OCBs controlled by own group
- Funds siphoned off to Mauritius/Europe and washed down through several accounts

Initial Public Offer (IPO) Scam- 2006

- In 2000 SEBI guidelines on Disclosure of Investors Protection Scheme(DIPS)

- 25% shares to Retail Individual Investors (RII)
- 25% shares to High Networth Individual (HNI)
- 25% shares to Non-Institutional Bidder (NIB)
- 25% shares to Qualified Institutional Buyers (QIB)
- National Securities Depositories Ltd. (NSDL) and Central Depositories Services Ltd. (CDSL) set up under

Depositories Act 1996.

- Central Depositories offer their services all over the country through Depository Participants (DP).

- All transactions in shares routed through DP's in which beneficiary owners (BO) open D-mat account.

- For opening D-mat A/c –

(a) Bank A/c.

(b) PAN No.

(c) Follow KYC norms of SEBI for:-

(i) Proof of Identity (POI).

(ii) Proof of Address (POA).

(iii) Proof of Income

Nexus Between DP, Bankers & Middlemen

- Fraudulently opened D-mat accounts of fictitious persons on the basis of forged bank documents and D-mat applications.
- D-mat account number used for submitting thousands of fictitious applications for allotment of shares in the RII category.
- Shares allotted to fictitious applications were transferred on forged Delivery Instructions Slips (DIS) to the D-mat account of middlemen before listing of shares.
- Listing prices much higher than allotment price, resulting in huge profit.

MERCHANTING TRADE TRANSACTIONS

- As per regulations MTT means that:-
- Import and Export leg is completed without goods touching the shores of our country
- Proceeds from exports must be utilized to square off the cost of imports within six months
- Importer and exporter must be the same party
- Coy. A imports goods from coy. B
- Payment released by Coy. A to Coy. B
- Coy. A shows expo of these goods to coy. C
- Coy. C is a front Coy. Of D, an agent of Coy.A
- Funds used by Coy. C for investments
- Profits/funds routed to D and not A
- Investments by Coy.C Tank
- Resultant losses to Coy. A

INDUSTRIES AT RISK DUE TO

ECONOMIC CRIMES:

HOSPITALITY SECTOr

October 10, 2015

Presented By

Anand Desai

Managing Partner

DSK Legal

ECONOMIC CRIMES

- Economic crime against businesses continues to rise globally.

- According to the Global Economic Crime Survey conducted by PwC; between 2011 and 2014 there has been a rise of 37% in economic crimes globally.

- 41% of the Hospitality Industry which was surveyed, stated that it suffered due to economic crime.

- It is likely the actual numbers and percentages are higher, as many instances may not be reported.

CRIMES IN THE INDUSTRY

- Skimming
- Purchasing fraud: Kickbacks and bid-rigging
- Theft of hotel property
- Theft of guest's property
- Cyber Crimes
- Tax Evasion
- Corruption in respect of land allocation, licences and approvals for hotels
- Money Laundering / Violation of Foreign Exchange Regulations
- Illegal activities carried out in Hotels

SKIMMING

- Considering the large amount of cash transactions, skimming is very common in the hospitality industry.

- Hotel employees in certain hotels can pocket cash payments made by guests, in part or full, and deny that the payment was made.

- This loss, has a great impact on the industry on the whole.

PURCHASING FRAUD

- Purchasing fraud is very common in the hotel industry. It can be divided into two heads: Kickbacks & Bid Rigging.

- Considering that hotels buy most items in bulk, they are generally entitled to large discounts from vendors.

- The hotel staff in collusion with the vendors has the bills inflated, sometimes just to a pre-discount value. The staff has the bill approved and money released, and subsequently pockets the discount that the hotel would have otherwise been entitled to.

- The same *modus operandi* is used for the bidding process.

THEFT OF HOTEL PROPERTY

- High value property such as paintings, artefacts and jewellery are frequently stolen from hotels / guests.

- *Fernand Leger Painting worth $350,000 was stolen at the Carlyle Hotel, Manhattan in 2011*

- *Andy Warhol painting worth $300,000 went missing from the W hotel in Hong Kong*

- Additionally, curtains, linen, toiletries, cutlery, pillows and slippers are commonly stolen.

THEFT OF GUEST'S PROPERTY

- Hotel guests often leave behind their jewellery, cash, passports and other valuables in their rooms.

- Guests are now bringing valuable items such as Ipods, Ipads, Laptops, etc. in addition to more traditional belongings such as clothes, watches, and jewellery.

- Such property is susceptible to theft as the hotel staff at all times has access to the room.

- Consequently, such valuables are sometimes stolen by hotel staff.

CYBER CRIME

- According to the Global Economic Crime Survey conducted by PwC, 25% of businesses reported being victims of Cyber Crime.

- There are various methods of cyber crime but the most common is online credit card fraud.

- Cyber criminals can hack into a company's customer database and steal large batches of guest credit card information that they then sell on the black market

- OR they can use the stolen credit card information to manufacture counterfeit credit cards, which they then use to fraudulently purchase goods or services

CYBER CRIME

A customer provides sensitive data through one or all of the following:

- Point of Sale Terminals
- ATMs
- Guest paperwork
- Reward Card Programmes
- Credit card details

DATA THEFT

- Hospitality businesses invest time and capital to efficiently collect and process data in order to improve sales, customer service and loyalty, and operations efficiency.
- All such businesses are vulnerable to system breaches.

SENSITIVE DATA

- The hotel smart key card, traditionally identified to control access for the guest rooms have become an information database.
- A hotel key card may now contain credit card details and other miscellaneous data that a guest may have submitted at the time of check-in.
- Further, most hotels follow a practice of asking their guests to return their key card at the time of check-out. Thus, practically handing over all their information.
- Additionally, there exists a possibility of the key card getting lost or stolen, resulting in decoding the data encrypted on the Magnetic Strip of the key card by a third person.

IDENTITY THEFT

Traditional modes of theft:

- Theft of wallets;
- Theft of a photocopy of the Identity Document.

Present day identity theft:

- Identity thieves are more interested in what's going over your hotel Wi-Fi connection than what's in your hotel room safe.

- In 2010, the Wyndham Hotels and Resorts; the operators of The Days Inn, Ramada and Howard Johnson Hotel chains reported that their networks had been compromised by hackers. As a consequence of which, an unknown number of guest names and credit card numbers were stolen.

CONSEQUENCES

- The immediate financial cost of a data breach is only part of the story.

- The consequential effects are a loss of customer trust and/or a tarnished reputation, which can be extremely difficult and expensive to rebuild. This is especially true for hotels and restaurants, which usually have high public profiles.

CONSEQUENCES UNDER THE IT ACT

- A person installing a voyeur camera in a hotel room, by means of which a person's body is photographed or filmed, and who communicates the same is liable to be prosecuted under Section 72 and 67.

- **72. Penalty for breach of confidentiality and privacy.** *Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record,*

book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

CONSEQUENCES UNDER THE IT ACT

- **67. Publishing of information which is obscene in electronic form**. *Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.*

TERRORIST THREATS TO THE HOSPITALITY INDUSTRY

- The hospitality industry is subject to constant terrorist threats in view of the premises being open to the general public at all times, thus resulting in a majority of people together under a common roof. This makes popular hotels and restaurants idle targets for terrorist attacks.

- The terror attacks on the Taj Mahal and Oberoi Hotel in Mumbai are examples of such terror attacks.

INSURANCE CLAIMS AGAINST TERROR ATTACKS

- The Indian Hotels Company (which runs the Taj Mahal hotel) and EIH Ltd (which operates the Oberoi and Trident hotel) have so far got Rs. 167 crore as insurance claim from General Insurance Corporation on account of the 26/11 terror attacks in Mumbai.

- This part-payment was given from the total claim of Rs 500 crore.

TAX EVASION BY HOTELS

- Conducting an investigation into tax evasion by a Hotel, an Investigating Officer stated:

- "Investigation revealed that taking advantage of one of the rules, the company was raising invoices of Rs.999 for visitors instead of the declared tariff of Rs. 3,500 to Rs. 16,500 amounting to tax evasion. Also, a batch of 50 people were given same rooms three times in 24 hours."

- Consequent to several arrests and convictions, wherein, service tax etc. collected from customers is not deposited with the government, the New Delhi government, in order to curb tax evasion, in July 2015, decided to put room tariff of all hotels from five-stars to budget hotels in the public domain.

- The hotels will only be allowed to charge what they declare as room tariff and any transgression will be acted upon.

FOREIGN EXCHANGE LAW VIOLATIONS

- The Indian Hotels Company Ltd. is being investigated for foreign currency transactions to the tune of around Rs. 600 crore. They are accused of setting up bank accounts in Switzerland, Oman, London without RBI's permission and diverting funds. The investigation commenced in April, 2015.

- According to the investigators, they received information that the erstwhile management of IHCL headed by Mr. Kerkar had indulged in various transactions in violations of provisions of FERA and FEMA.

FOREIGN EXCHANGE LAW VIOLATIONS

- In June, 2015, the Enforcement Directorate as part of its probe into suspected foreign exchange violations in the funds received by Ananda Heritage Hotels Private Limited, a company controlled by Lalit Modi.

- The Enforcement Directorate served a show-cause notice on the Sahara Group and its chief Subrata Roy, seeking explanations for alleged violation of foreign exchange rules involving an overseas direct investment of about Rs.3,662 crore in 2010.

- Enforcement Directorate investigations have revealed that the amount was channelised by Sahara India companies for the purchase of Grosvenor House Hotel from the Royal Bank of Scotland without following mandatory guidelines.

CORRUPTION LEADING TO LAND ALLOTMENT FOR HOTELS

- According to the CAG report for the period ended March, 2012:

- In the case of the Hotel; ITC Sonar Bangla, the General Administration Department disregarded the zonal regulations and also charged premium at a lower rate of Rs.35 lakh per acre against the market value of Rs. 1.50 crore, which resulted in a loss of revenue of Rs. 5.90 crore.

- The CAG also pulled up the GAD on the issue of the Hotel South Pac's land reportedly being taken possession by the son of a Minister in the Unit-8 area of the city in violation of the land use zone and its conversion being done in a hasty manner within 56 days.

CORRUPTION LEADING TO LAND ALLOTMENT

- Further, in another observation under the CAG report; 6.832 acres of forest land was allotted in case of four lessees including 3.237 acres of Hotel Mayfair and Resorts Private Limited at Jayadev Vihar without obtaining

requisite forest clearance from the Union Ministry of Forest and Environment in favour of the respective agencies.

CORRUPTION TO ATTAIN LICNCES AND APPROVALS

- Starting and running Hotels, Restaurants, Bars etc. require several licences and approvals from various government authorities.

- Depending on the size of the establishment, 30 – 80 Licences and Approvals might be required.

CORRUPTION TO ATTAIN LICENCES AND APPROVALS - KERALA BAR BRIBE SCAM

- Around the end of October 2014, the hotel and bar owners association's working president, alleged that he paid Rs.1 crore to Finance Minister K.M. Mani, for a government decision in favour of the bar owners.

- A FIR was filed against Mr. Mani based on preliminary investigations into allegations that he accepted Rs. 1 crore as part of a deal to renew the licenses of 418 "sub-standard" bars that were closed in the state last year.

- The Vigilance Court has reserved the verdict on the petition seeking further investigation into the Bar bribery case involving K. M .Mani, on October 29, 2015.

MONEY LAUNDERING

- The Hospitality Industry, being an industry where cash is legally tendered, attracts opportunities for money laundering.

- Large amounts of cash are paid to Hotels not only by way of settling room tariffs, food bills etc., but also, banquet payments which are generally substantial in nature.

- Income Tax officials raided casinos and other properties of two biggest gaming companies, Delta Corp and Pride Group in April, 2014.

- The raids were carried out by the IT department over allegations of money-laundering and tax evasion by the two companies.

- The raids were carried out by tax authorities on a tip-off by unnamed informants indicating that large unaccounted cash transactions were carried out by casinos and that high rollers used casinos to transact in black money.

- The Enforcement Directorate has found the Rose Valley group to have systematically engaged its various companies to launder legitimate investor funds and ploughed them into purchasing realty assets and fund its own jewellery, entertainment and hospitality businesses.

- Mohammad Fasih, chairman and managing director of the Showman Group was taken into custody by the Economics Offences Wing for siphoning off crores of rupees belonging to the South Indian Education Society Trust and government bodies.

- Fasih during questioning revealed that he had invested part of the scam money in his hotel business in Goa.

ILLEGAL ACTIVITES IN HOTELS

- In *Shri Ganga Bahadur Thapa Vs. The State* 1997 Bom CR (Cri) 839, the Bombay High Court convicted the accused under section 20(b)(ii) of The Narcotic Drugs and Psychotropic Substances Act, 1985, at Mapusa Hotel Safari. The police recovered 2,860 Kgs. of charas from the room No. 10 of the hotel which he was occupying.

- The Court sentenced the accused to suffer rigorous imprisonment for a period of 10 years and to pay a fine of Rs. 1,00,000/-.

- The accused, while in custody, disclosed that they had come from Himachal Pradesh and were staying at a Hotel at Mapusa called Safari where they had brought the charas and kept.

- Recently, five policemen in Chennai, have been suspended for gambling in a hotel room and attacking the manager.

- The policemen booked two rooms in a hotel on Kennet Lane on January 3, 2015 and invited their friends to join them. A gang of 10 people were drinking, gambling, creating a ruckus in the room, and disturbing other guests.

- The hotel manager went to the room and asked them to refrain from gambling. The enraged policemen started an argument with him. When the manager did not back down, they attacked and threatened him.

- On February 13, 2015 a high-profile gambling and sex trade racket at a three-star hotel in Ghaziabad was busted, resulting in the arrest of 72 persons, including 6 women.

- The accused have been booked for drinking without liquor permits, gambling and indulging in sex trade. The six women were booked under the Prevention of Immoral Traffic (Prevention) Act, 1956.

- The Ghaziabad police recovered about Rs 10 lakh and seized 19 cars and three licensed pistols.

ILLEGAL ACTIVITES Vis-à-Vis RIGHT TO PRIVACY IN HOTEL ROOMS

- On August 6, 2015, a team of police officers led by DCP Vikram Deshpande, raided several lodges, resorts, two-star hotels and beaches in Madh Island and Aksa beach in the western suburbs of Mumbai.

- The police arrested 13 couples and 35 others for indecent behaviour in public and 3 women on charges of immoral trafficking under the Prevention of Immoral Traffic Act, 1956. A deposit of Rs. 1,200 along with an

undertaking to appear before the local magistrate was taken from each of the 61 individuals.

- Recently the police has admitted to committing a "mistake" by conducting these raids and an inquiry has been sought.

Thank you.

Brief on Insurance fraud monitoring framework

- Financial Fraud poses a serious risk to all segments of the financial sector. Fraud in insurance reduces consumer and shareholder confidence; and can affect the reputation of individual insurers and the insurance sector as a whole
- Pre-revised ICP 27 on Insurance Frauds requires insurers to have a mechanism to deter, detect and mitigate risks arising from frauds.
- Major focus of ICP is on:
  - Sharing fraud details among the insurance companies
  - Report frauds to appropriate authorities
- Considering the importance of having appropriate risk mitigation measures in the insurance sector, IRDA had earlier mandated Risk Management Committee under the Corporate Governance Framework. A certain level of risk mitigation measures are also in place in the form of regular audits on insurance companies' financials.
- Arising out of the concerns raised in the Financial Sector Assessment Program (FSAP), it was decided to lay down a detailed framework for Insurance Fraud Monitoring. A circular was issued on 21st January 2013.
- Detailed deliberations with various insurance companies, both life and general insurance councils have been carried out before the framework was formulated. This is to ensure that the different threats/vulnerabilities of fraud risks which vary with various lines of business are adequately taken care of. As the insurance companies are in a better position to know the threats they face in each lines of business, ample scope is given for the insurers to lay down the fraud monitoring framework which suites them more.
- We realized that the most important component for an effective fraud monitoring framework is 'sharing of fraud related information' among the

insurers, which we understand is not happening, as expected, currently. To address this aspect, IRDA has mandated sharing among the insurers in the platform of respective councils. Insurers again have been given freehand to decide the modes and methods of sharing like, what kind of information is to be shared, how it can be shared etc.,

- The circular broadly categorises the possible frauds in the insurance sector into policyholder/claim fraud; internal fraud; intermediary fraud. Care is taken to cover various areas which are currently bothering the insurance sector.
- Need for Board approved Anti-fraud policy covering aspects like procedures to be in place, coordination with law enforcement agencies, reporting channels, periodic reporting to the Authority etc.,
- The circular would be effective from the year 2013-14. Appropriate framework should be however, laid down by 30th June 2013 and a compliance certificate is to be filed with IRDA

INSURANCE FRAUDS INTERNATIONAL VIEWS-IAIS/FSA…

ICP 27*-FRAUD

- The supervisory authority requires that insurers and intermediaries take the necessary measures to prevent, detect and remedy insurance fraud

- 7 Essential Criteria
  - Supervisory authority to have powers and resources
  - Legislation addresses insurer fraud
  - Claims fraud is a punishable offence
  - Supervisory authority requires insurers/intermediaries to ensure high standards of integrity of their business

- Insurers/intermediaries to have effective procedures and controls to deter, detect, record and as required, promptly report fraud to appropriate authorities
- Supervisory authority promotes the exchange of information between the insurers
- Supervisory authority co-operates with other supervisory authorities in countering fraud.

(*revised ICP 21 - Countering fraud in Insurance)

IAIS- APPLICATION PAPER ON FRAUD

Application Paper* on Deterring, Prevention, Detecting, Reporting and Remedying Fraud in Insurance-September 2011

- Describes fraud in insurance
- Red flag indicators for various types of frauds
- Supporting measures and procedures
- Examples and cases of types of frauds

(*replaces the IAIS guidance paper No. 12 (October 2006) on preventing, detecting and remedying fraud in Insurance

DEFINITION (IAIS GUIDANCE NOTE)

An act or omission intended to gain dishonest or unlawful advantage for a party committing the fraud or for other parties

Which may be achieved by means of:

- Misappropriating assets
- Misrepresentation of facts
- Abusing a fiduciary relationship

TYPES OF FRAUD

- Internal Fraud- by staff

- Policyholder fraud/claims fraud-in purchase and/or execution of an insurance product

- Intermediary fraud

- Fraud by contractors/suppliers excluded

FRAUDSTERS' PROFILE

- **Opportunity Fraudsters**

e.g., They imagine that insurers have limitless funds and might find it acceptable to make up claims in order to recover the costs of premiums paid in previous years when there have been no claims**.**

- **Professional Fraudsters**

e.g., Organised crime involving a group of persons capable of committing complex and extensive frauds

RISK MANAGEMENT OF FRAUDS

- Corporate Governance of the Board:
  - Proper policies, procedures and controls to prevent and detect
  - Separate fraud management function
  - Can be part of risk or audit committee
- Board and Senior Management responsible
- Address fraud risk in mission, strategy & business objectives

RISK MANAGEMENT OF FRAUDS CONTD…

- Regularly review anti-fraud policies, procedures and controls
- Fraud Investigation-expertise in legal, forensic, IT, auditing and medical expertise-in-house or outsource
- Board/Sr. Mgt to receive reporting
- Clear policies for reporting suspicions of fraud to law enforcement agencies
- Information sharing within the organization

INTERNAL FRAUD

- Vulnerability:
  - Complexity
  - Speed of Innovation
  - Remuneration/promotion policies
  - Weaknesses in internal controls
  - Economic climate and business situation
- Warning Signs:
  - Staff working late
  - Senior staff resigning unexpectedly
  - Unexplained wealth of or living beyond apparent means by Board members/senior level executives
  - Customer complaints
  - Rising costs with no explanation etc.,

INTERNAL FRAUD-CASES

Case 1 – Theft of information

- Employee print confidential customer data
- Investigation reveals -employee had been offered money for the information.
- Reported by other employee

Case 2 – Intellectual Property Fraud; Computer Technician gets seven years in jail for stealing

- Miss T. was a computer data entry technician for an insurer.
- She issued 42 claim drafts, for in total more than $207,000 and arranged mailing by computer from the insurer to T. at three separate addresses.
- She was arrested and charged.

INTERNAL FRAUD-CASES

Case 3 – Claims supervisor found guilty of theft

- Mr S. was found guilty on theft for making fictitious claim payments to non-existent people.

- Mr S was creating claimants, manufacturing claims, authorizing payments and negotiating company drafts with the help of a niece, a teller at a local savings and loan association.

- Mr S. would call his niece each time he had worked the scheme to the point of draft issuance, and tell her the claimant would be in shortly, and ask her assistance in cashing the draft.

INTERNAL FRAUD-PREVENTIVE MEASURES

- Creating culture/atmosphere
- Issuing procedural manuals
- Adequate supervision of management
- Pre-employment/in-employment screening
- Requiring periodical job rotation
- Separation of functions susceptible to conflict of interest
- Adequate Internal controls
- Clear reporting lines/communication procedures etc.,

POLICYHOLDER FRAUD/CLAIMS FRAUD

Examples

- Reporting/claiming of fictitious damage/loss
- Exaggerating damages/loss covered by the insurance
- Misrepresenting a fact
- Misrepresentation by an impostor
- Staging occurrence of incidents causing damage/loss covered

Mitigation measures:

- Establish client acceptance policy
- Client acceptance procedures-identify/verify
- Inform potential/existing clients about their anti-fraud policies.
- Claim assessment procedures

POLICYHOLDER/CLAIM FRAUD-CASES

Case 1 – Staging car accidents by criminal gangs

- A criminal group will arrange for a fee of £500 an accident for the fraudster.
- One of the criminals will use the identity documents of the fraudster to impersonate him.
- The fraudster will subsequently file an insurance claim.
- The criminal group would also provide a fake medical report for a whiplash claim.
- Apparently, the average payout on a staged accident was £3,000, often with a £2,500 claim for whiplash damage.

Another modus operandi:

- A fake car crash could be staged for less than £2,000.

- Two drivable cars could be bought to stage a crash for £1,000. For an extra £800 a customer could buy £500 of comprehensive insurance, and another £300 of third party cover.
- After a fake crash had been staged all participants could claim £2,500 for whiplash injury and £5,000 for the written-off cars, fake car hire and loss of earnings. This way, fraudsters could collect on a £26,000 claim.

POLICYHOLDER/CLAIM FRAUD-CASES

Case 2 – False mobile phone thefts

- In Britain the police force receives 160 false reports of mobile phone thefts a month, which costs it £1 million a year to investigate.
- The National Mobile Phone Crime Unit estimates that between 15-20 per cent of mobile phone theft reports in the UK are false.
- Police suspect that false claims are sometimes
    - encouraged by unscrupulous mobile phone shop staff looking for extra commission.
    - someone who has lost their phone will falsely report it as stolen in order to claim on their insurance.

Case 3 – Arson by a drug syndicate

- A syndicate of drug barons bought a gold refining plant in Florida
- Insured with Lloyds',
- Burnt it down partly in order to launder "dirty" monies.

INTERMEDIARY FRAUD

- Examples:
    - Withholding premium collected from a policyholder until a claim is reported
    - Insuring non-existent policyholders
    - Colluding with policyholders to commit claims fraud
- Warning signs:
    - Request for payment of commission immediately/in advance
    - Small portfolio but high insured amounts
    - Personal or other close relationship between the client and the intermediary
    - Frequent changes of address or name of intermediary etc.,

INTERMEDIARY FRAUD-CASES

Case 1 – Backdated cover

- Intermediary was backdating motor insurance policies to give motorists the appearance of insurance coverage after an accident had already occurred.
- In exchange for this illegal activity, the agent/broker demanded a fee.
- Some applicants were charged up to $3,000 for a backdated policy. –three insurers were affected

Case 2– A bogus insurance programme

- An intermediary based in the US collected $3.8 million in a nationwide bogus insurance programme.
- The intermediary was arrested and charged on 63 counts relating to the sale of thousands of fake insurance policies throughout the US.

INTERMEDIARY FRAUD-CASES

Case 3 – Premium for $22,000,000 in insurance for hotels

- Mr L, an insurance intermediary, accepted a premium of $408,570 to place $ 22,000,000 in property and liability insurance for a hotel group.
- One cheque was issued for the entire premium, on behalf of the six hotels.
- Mr L. deposited this cheque into his account and used approximately $77,000 of it to buy some insurance for the hotels.
- Unfortunately for the hotels, Mr L. had a lot of personal debts.
- He used the “change” (about $170,000) to buy himself a boat and a condo.

- L. admitted manufacturing and altering several documents to indicate the proper amount of coverage for the premium paid by the hotel group.

INTERMEDIARY FRAUD-PREVENTION & DETECTION

- Screening mechanism for appointments
- Check financing soundness of the prospective intermediary
- Fit & proper standards for the Board/Senior Management of the intermediary
- Effective sanction policy for non-compliance
- Periodic audit
- Avoid intermediary involvement in certain operational procedures like delivery of documents to policyholders directly, no cash acceptance by intermediary etc.,

FRAUDS LEADING TO MONEY LAUNDERING

- Life Insurance- Vulnerable products:
  - Unit-linked or with profit single premium contracts
  - Single premium life insurance policies

- Non-Life-Vulnerable areas:
  - Cancellation of policies for the return of premium by an insurer's cheque;
  - Overpayment of premiums with a request for a refund of the amount overpaid;
  - Under-insurance

INTERNATIONAL PRACTICES -UK-FSA

- Insurer/intermediaries to establish and maintain effective systems and controls for countering financial crime
- Monitoring through desk based approach/on-site visits
- Financial crime specialists provide support and technical advice
- The top 100 high impact firms receive targeted and regular scrutiny from their supervisors.
- Wide range of administrative sanctions against both individuals and firms.

INTERNATIONAL PRACTICES -UK-FSA CONTD…

- Dedicated Financial Crime and Intelligence Department within the Enforcement and Financial Crime Division.
- Regulation allows the FSA to disclose confidential information to any person (including the FIU) –in UK & elsewhere
- Wide range of MoUs with domestic and international authorities.
- Firms to notify the FSA if it becomes aware of events that may adversely affect the firm.
- FSA maintains internal databases which contain details in respect to fraud and those committing fraud.
- Substantial fines have been imposed, prompting the whole industry to implement corrective action.

INTERNATIONAL PRACTICES-USA

- The NAIC model law Insurance Fraud Prevention Model Act sets out :
  - prohibition,
  - gives investigative powers,
  - establishes mandatory reporting to the regulator,
  - provides for creation of fraud prevention units (fraud bureaus); and
  - requires companies to take antifraud initiatives to detect, prosecute and prevent fraudulent insurance acts.

- Insurers to have anti-fraud plan which must be submitted to the commissioner

INTERNATIONAL PRACTICES-USA CONTD…

- Insurers to report to departments external, internal and suspected claims fraud.

- NAIC provides for use of consumers and insurers an online system-Online Fraud Reporting System (OFRS).

- The National Insurance Crime Bureau (NICB) a NPO supported by P&C insurers works with law enforcement agencies to facilitate identification, detection and prosecution of insurance crime, managing database on insurance crime, organizes training /awareness programmes

INTERNATIONAL PRACTICES-ITALY

ISVAP -the regulator for insurance companies :

- Enforce rules for internal controls of insurers/ ethical standards of insurers/intermediaries
- Is authorized to co-operate with law enforcement officials and other supervisory authorities (both within/outside the country) with respect to fraud

- Governing law for frauds is criminal code
- No specific requirements on insurance companies for effective prevention/detection mechanisms for frauds

INTERNATIONAL PRACTICES-SPAIN

- Insurance fraud addressed by General Law
- Considered as Criminal activity
- Supervisory authority
  - Has powers to enforce regulations in the area
  - Report this kind of activity to competent authorities
  - Collaborate with other local/foreign authorities

INTERNATIONAL PRACTICES-SPAIN CONTD..

- Supervisory authority reviews internal controls in place to detect, prevent fraudulent activities

- The Spanish Association of Insurance and Reinsurance Institutions (UNESPA) - the Business Association for the Insurance Sector

    - has MoUs with various departments for cooperation mechanism

    - Supports industry on prevention/control of insurance frauds.

INTERNATIONAL PRACTICES-SWEDEN

- The Swedish Financial Supervisory Authority (FI)- no formal authority to establish and enforce regulations to combat fraud

- Fraud generally addressed in the Criminal Code (which covers insurance fraud)

- FI has no legal obligation to require insurers to report fraud to appropriate authorities

- Non-binding regulations expect insurers to report events that may jeopardize its stability or policyholders' assets

- Some checks during on-site inspections

- Swedish Insurance Federation has organized counter-fraud activities

- Industry has also organized a common claims database

INTERNATIONAL PRACTICES-GERMANY

- Insurers to report to BaFin (Federal Financial Supervisory Authority) any case of fraud/possible fraud
- Insurance fraud addressed indirectly via internal controls and compliance rules for the insurance undertakings
- Governed under Criminal Code
- German Insurance Association
    - Provides its members with training on combating fraud
    - Organized meetings for exchange of experiences
    - Drawn up advice for its members on fraud prevention
    - Manages a database to help combat fraud.

STATUS ON DATE-SFIO

- Serious Frauds Investigation Office:
    - a multi-disciplinary organization under Ministry of Corporate Affairs,
    - experts in accountancy, forensic auditing, law, information technology, investigation, company law, capital market and taxation
    - for detecting and prosecuting or recommending for prosecution white-collar crimes/frauds.
    - normally take up for investigation only such cases
        - having inter-departmental and multi-disciplinary ramifications ;
        - substantial involvement of public interest;
        - Investigation contribute towards improvement in systems, laws or procedures and those received from Department of company Affairs.

PREVAILING CHECKS IN INSURANCE SECTOR

- Corporate Governance Guidelines
    - Mandates Risk Management Committee & Audit Committee
    - While Blowing Policy

- AML/CFT guidelines:
    - Customer acceptance policy
    - Customer identification policy (KYC Norms)
    - Screening mechanisms for employees/agents
    - Internal audit-exception reporting to Audit Committee

PREVAILING CHALLENGES IN INDIA

- There is no Indian law specifically dealing with insurance fraud
- No specific requirement for insurers/ intermediaries to have fraud detection/ mitigation mechanism
- Interest in detecting a fraud is limited to repudiation of liability
- No structured manner of exchange of information among insurers
- No reporting .

This paper was prepared by the Insurance Fraud Working Group of the Market Conduct Subcommittee in consultation with IAIS Members and Observers.

1. The purpose of this paper is to provide information on how fraud can occur within the insurance sector, so that the potential risk of fraud can be identified and reduced. It supplements ICP 21 on *Countering fraud in insurance* and the accompanying standards and guidance, which apply to insurance supervisors.

2. Within this context this paper provides information that can be used by insurers (including reinsurers) and insurance intermediaries. References to insurers should be read to include intermediaries.

3. Insurers should assess their own vulnerability and implement effective policies, procedures and controls to manage the risk of fraud. They should ensure that their anti-fraud policies, procedures and controls apply to all their branches, including those located abroad. Insurers should therefore adopt a risk-based approach when addressing fraud on the basis of the fraud risk management referred to in section 2.3. Groups should make such assessments from the group perspective, assessing the differing vulnerabilities throughout the group, and ensure that effective policies, procedure and controls to manage the risk of fraud are in place throughout the group.

4. This paper is also applicable to reinsurers – including sections 2 and 6 – and the measures discussed should be implemented on a risk-sensitive basis (for example, depending on the risk profile and the nature, scale and complexity of their business). Reinsurers should apply section 3 on internal fraud in its entirety and, where they use intermediaries, section 5 as much as possible. With respect to section 4 on policyholder fraud and claims fraud, reinsurers should take into account policies, procedures and controls to manage fraud risk that their ceding insurers have in place as part of the reinsurer's own risk management.

5. Reinsurers can reduce their exposure to fraudulent claims from ceding insurers and reinsurance intermediaries by understanding the fraud risk management systems these counterparties have in place. Staff of the ceding insurer may be colluding with third parties in a scheme intended to defraud the reinsurer – for example, scheming with policyholders, they could add costs not related to the claims recovery.

6. Insurance supervisors may also wish to consider the information contained within this paper, in order to assist them in determining how best to apply anti-fraud measures in respect of their own insurance industry.

2 Fraud risk in insurance

7. Fraud comes in all shapes and sizes. It may be a simple act involving one person or it may be complex operation involving a large number of people from within and outside the insurer. This paper considers the following types of fraud:

(a) Internal fraud – Fraud against the insurer by a Board member, senior manager or other member of staff on his/her own or in collusion with others who are either internal or external to the insurer

(b) Policyholder fraud and claims fraud – Fraud against the insurer in the purchase and/or execution of an insurance product by one person or people in collusion by obtaining wrongful coverage or payment.

(c) Intermediary fraud – Fraud by intermediaries against the insurer, policyholders, customers or beneficiaries.

8. There are other types of fraud that affect insurers, which are not covered in this paper, such as:

- fraud committed by contractors or suppliers that do not play a role in the settlement of insurance claims
- fraud by misrepresentation of insurance cover to attract investors, obtain favourable loans or authorisations or other types of favourable decisions from public authorities.

2.1 Fraud triangle

9. There are three basic components that contribute to the occurrence of fraud, namely:

a) motive/incentive

b) opportunity

c) rationalisation.

These basic components are often known as the fraud triangle.

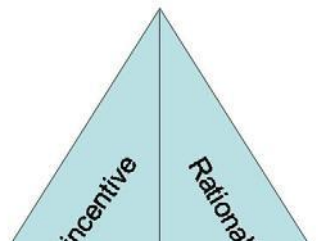


Figure: Fraud triangle

10. People commit fraud for a variety of reasons. They could, for example, have financial problems or be under pressure to meet unrealistic business objectives. Insurers should be aware of the potential for these conditions to exist and look for signs of possible fraud.

11. Fraudsters need to have the opportunity to commit fraud. They are more likely to act when they think the likelihood of detection is small. Therefore insurers should have proper policies, procedures and controls to both prevent fraud from taking place and, if fraud does take place, to detect it.

12. Rationalisation is the mental process of justifying the fraud. For example, people may commit fraud because they:

- are dissatisfied with an insurer as an employer
- perceive an entitlement to compensation because of premiums paid
- take an "every one does it" attitude
- are copying the behaviour of others in the insurer, such as the Board or Senior Management.

Also, public attitude regarding fraud in insurance does not deter fraud as many people see such fraud as a victimless crime.

13. The possibility of fraud is significantly reduced if the proper checks and balances exist. In designing appropriate policies, procedures and controls, insurers should be aware that their vulnerability to fraud is influenced by the business environment affecting the

insurers operations, as well as by the integrity and personal conditions of the Board members, senior managers and other staff.

2.2 Profiles of insurance fraudsters

14. There are two general profiles of fraudsters:

(a) The "opportunity" fraudster: an opportunity fraudster is normally a

law-abiding person who sees an opportunity to commit fraud. For example, this type of fraudster might imagine that insurers have limitless funds and might find it acceptable to make up claims in order to recover the costs of premiums paid in previous years when there have been no claims. With regard to internal fraud the fraudster might, for example, falsify expenses or the financial accounts of an insurer for his/her benefit.

(b) The "professional" fraudster: a professional fraudster earns or complements his/her income by committing fraud. He or she may continue committing fraud until detected and may target a number of insurers. An extension of the professional fraudster profile is organised crime involving a group of persons capable of committing complex and extensive frauds. The fraudulently obtained funds may be used to finance other criminal acts.

2.3 Fraud risk management by insurers

15. Insurers should be constantly vigilant in deterring fraudsters. As part of their corporate governance the Boards of insurers should recognise and understand the risks of fraud to their organisation, including the potential types and impact of fraud. By understanding the risks of internal, policyholder, claims and intermediary fraud, insurers can decide which procedures and controls can be implemented effectively and efficiently to manage these risks.

16. The Board and Senior Management are responsible for fraud risk management. Fraud risk management should be a component of every insurer's risk management framework.

17. Insurers should address fraud risk when establishing their mission, strategy and business objectives. The overall policy should be consistently implemented in departmental objectives. It should be reflected in the relevant operational procedures and controls, for example, for:

- developing products
- accepting clients
- hiring and firing management and staff
- outsourcing
- handling claims
- dealing with intermediaries.

18. For this purpose it is essential that an insurer should:

- establish and maintain a sound control environment through policies, procedures and controls. Insurers should require high standards of integrity in its Board, Senior Management and other staff as part of

their business values and a proper organisational culture.

- demonstrate a proper support by the Board and Senior Management ("tone at the top"), and overall communication of these values throughout their entire organisation.
- set realistic business objectives and targets and allocate sufficient resources for the Board, Senior Management and other staff to meet them.
- organise and collect management information with respect to fraud in insurance, making it available in a timely manner for the Board and Senior Management to monitor developments and take appropriate action. This information should be used to periodically evaluate the effectiveness of policies, procedures and controls and make changes where necessary.
- establish and maintain an adequate and independent audit function to test risk management, procedures and controls.

19. The extent and specific form of policies, procedures and controls needed to prevent and detect fraud should be determined following a risk analysis. Relevant factors to consider include:

- size of the insurer
- group, responsibility and organisational structure
- products and services offered
- payment methods used for premiums and claims
- types of policyholder, and
- market conditions.

20. Fraud risk can be impacted by the insurer's method of distribution, for example, direct writing or use of tied agents or independent brokers. The amount of contact with the client, involvement of the insurer's staff and reliance on third parties can differ depending on the distribution method used and this will influence the nature and size of the risk of fraud. Special policies, procedures and controls may be needed when new technologies, such as the internet, are used to distribute products.

21. If warranted by their risk profile and by the nature, scale and complexity of their business, insurers should consider introducing a separate fraud management function. This function would be responsible for the design of, and compliance with, the insurer's anti-fraud policies, procedures and controls, as well as any fraud investigations. It could maintain the insurer's fraud statistics and related management information. In addition, this function could coordinate the information exchange with other insurers and financial institutions and with third parties, such as law enforcement authorities. If established, the fraud

management function would need to:

- have the requisite authority
- have sufficient resources
- be able to raise issues directly with the Board, or board risk or audit committee, and
- be able to maintain confidentiality.

22. As part of their fraud risk management, insurers should have a set of measures and procedures to be able to respond adequately and, if necessary in emergency situations, quickly to (suspected) cases of fraud. These measures and procedures would include possible fraud investigation.

23. Fraud investigations require a variety of possible areas of expertise (for example: legal, forensic, IT, auditing and medical expertise). Insurers should ensure that they have the relevant expertise either in-house or by outsourcing fraud investigations to appropriate third parties, provided that the quality of fraud investigations and the confidentiality of information are not compromised by the outsourcing.

24. The Board and Senior Management should ensure that the nature and frequency of reporting, as well as the time allocated for considering fraud matters, is sufficient since they are responsible for establishing and implementing the requisite policies, procedures and controls. Information about fraud, such as trends and profiles of fraudsters, should be shared and known throughout the insurer. Possible indicators of fraud (or red flags[1]) can therefore be identified early by putting together different pieces of information.

25. Insurers should regularly review their anti-fraud policies, procedures and controls taking into account the dynamic nature of fraud. When an insurer has been exposed to fraud, it should use the incident to identify "lessons learned" and adjust its policies, procedures or controls to minimise the risk of the fraud recurring.

3 Internal fraud

3.1 Internal fraud risk

26. As part of their management of operational risk, insurers should consider the effect on staff morale as well as the potential for financial losses resulting from internal fraud. Internal fraud also poses a reputational risk to insurers. Severe cases could precipitate economic ruin of insurers. (See Appendix A – Examples and cases of (alleged) internal fraud in insurance.)

27. Factors influencing an insurer’s vulnerability to internal fraud include:

- its complexity – internal fraud is more likely to occur in insurers with a complex organisational structure, where there is increasing

compartmentalisation of responsibilities or lack of identification with the insurer.

- its speed of innovation – the speed of modern commerce, product development and computerisation, promote opportunities for fraud.
- its remuneration and promotion policies – the incentive to commit fraud may be greater if an employee's pay and status depend on meeting certain targets.
- weaknesses in internal control, including concentration of decision making in a small number of individuals.
- the economic climate and business situation – phases of instability within an insurer such as mergers and acquisitions or takeover bids may provide unexpected opportunities for fraud. Fraud is more likely to occur when an insurer's control systems and environment are not sufficiently robust.

Generally, internal fraud occurs on all levels, including at the level of the Board and Senior Management. The higher the level at which the fraud is committed the higher the likely financial loss and reputational damage.

28. Employees pilfering cash or insurer's resources – such as equipment, stock, or information – represent the most conventional fraudulent behaviour. However, corrupt employees also engage in far more costly schemes. These include bribery and kickbacks. A bribe usually "buys" something, for example, the influence of the recipient who makes the business decision. Although not as common as other types of fraud, commercial bribery schemes are usually very costly and involve collusion between employees and third parties. Typically, these schemes involve receiving kickbacks or commissions from a supplier as a reward for awarding the contract. This type of fraud is particularly difficult to detect, since the kickback is paid directly from the supplier to the employee and does not go "through the

[1] an indicator that suggests the need for more detailed investigation of a fact, event, statement or claim. It may – especially in combination with the occurrence of other red flags – indicate potential fraud.

books" of the insurer. Such corrupt practices often escape detection, unless exposed by other employees, vendors or other third parties.

29. Typical warning signs for internal fraud are:

- senior managers or other members of staff working late, who are reluctant to take vacations or who seem to be under permanent stress
- Board members, senior managers or other members of staff resigning unexpectedly

- marked personality changes of Board members, senior managers or other members of staff
- unexplained wealth of or living beyond apparent means by Board members, senior managers or other members of staff
- sudden change of lifestyle of Board members, senior managers or other members of staff
- key managers or members of staff having too much control and/or authority without oversight or audit by another person, or who resist or object to (independent) review of their performance
- Board members, senior managers or other members of staff with external business interests and/or cosy relationships with third parties giving rise to conflicts of interest. For example, a disproportionate amount of business or other forms of "support" may be granted to third parties who are not at arm's length from managers or members of staff
- customer complaints
- missing statements and unrecognised transactions
- rising costs with no explanation.

30. The existence of these warning signs or indicators does not mean that internal fraud has occurred or will occur. Nevertheless, insurers should be looking out for these warning signs or indicators, particularly when more than one occurs. Appendix B – Potential internal fraud indicators – red flags presents an extended list of potential risk indicators.

3.2 Internal fraud deterring and prevention

31. Measures to deter and prevent internal fraud are essential for controlling this risk. They also help the insurer avoid the negative effects of adverse publicity and supervisory attention or intervention, if a serious case of internal fraud is detected.

32. Insurers should identify both the processes of their organisation that are vulnerable to internal fraud and the consequent individual internal fraud risks.

33. Insurers should raise awareness of the potential for internal fraud within their organisation. For example, the Board, Senior Management and other staff should be provided with guidance on potential internal fraud indicators and training on deterring preventing, detecting, reporting and remedying internal fraud (see section 6.1 on training).

34. Fit and proper standards should be established for members of the Board, senior managers and other staff that are appropriate for their position and responsibilities. Equivalent standards should be set for third parties hired by

insurers to perform activities in high risk areas.

35. The initial and on-going assessment of the fitness and propriety of management and staff should include the verification of identity, personal information and background.

36. Personnel records should be complete and contain all information on the recruitment of Board members, senior managers and other staff. Records should be retained for an adequate period of time after the person in question has left the insurer.

37. During recruitment, insurers should be aware that applicants could provide false information, such as false employment history, false references and certificates or false identity.

38. Preventive policies, procedures and controls include (among other things):

- creating a culture and atmosphere which place value on the integrity of the Board, Senior Management and other staff, which foster their identification with the insurer, and which put value on staff that call colleagues to account about matters of misconduct
- issuing an office manual and internal guidelines on ethical behaviour for management and staff
- maintaining adequate supervision of management and other staff
- performing pre-employment and in-employment screening of permanent or temporary management and staff
- establishing clear responsibilities in documented job descriptions or role statements
- requiring periodical job rotation and mandatory vacations for management and staff in fraud sensitive positions
- eliminating potential conflicts of interest between the insurer, Board members, senior managers and other staff
- separating or dividing any function that may cause or be susceptible to conflicts of interest
- observing the four eyes principle (involvement of more that one person in decision making or other material activities for reasons eg of validation, proper governance, transparency and control)
- adequate segregation of functions
- establishing efficient physical and procedural safeguards over the use, handling and availability of cash, other assets and transactions as well as of information systems
- arranging for cash and money flows to be dealt with by more than

one person

- establishing clear reporting lines and communication procedures
- establishing internal complaints procedures for disgruntled management and staff
- establishing a transparent and consistent policy in dealing with internal fraud by Board members, senior managers and other staff, including policy on notification to the relevant law enforcement agency
- establishing a clear dismissal policy for internal fraud cases in order to deter other potential perpetrators.

3.3 Internal fraud detection

39. Internal fraud detection supplements internal fraud prevention. It demonstrates the effectiveness of preventive policies, procedures and controls. It should be borne in mind that the ways of committing fraud are limited only by the imagination of the individual(s) – this

human factor" makes the detection of internal fraud particularly difficult and therefore makes prevention of major importance.

40. Internal audits are a successful tool for detecting internal fraud. Therefore, insurers should carry out risk-based internal audits at appropriate intervals. In order to be effective audit staff needs timely access to information and technological tools to audit computerised systems and files.

41. An internal audit function should be independent from the day to day activities and accountable to the Board or an equivalent body. If appropriate, and while still retaining accountability for the work undertaken, the insurer could assign the audit function to an independent external organisation. Internal audits should be applied to the Board and all management and staff levels. They should include all the insurer's business lines and processes.

42. Insurers should encourage management and staff to report irregularities. They can increase the chance of detecting fraudsters by establishing confidential reporting mechanisms (see 6.2). Confidential reporting mechanisms demonstrate to staff that the insurer is intolerant of fraud.

43. Some insurers have a policy on disclosure of information on potential fraud or other unlawful behaviour (for example, whistle blowing). The exposure and reporting of fraud and abuse committed by a Board member, senior manager or other member of staff can be a valuable source of information for managing internal fraud.

44. Exit interviews when a Board member, senior manager or other member of staff leaves the insurer can provide useful information for countering fraud.

4 Policyholder fraud and claims fraud

4.1 Policyholder fraud and claims fraud risk

45. As part of their management of operational risk, insurers should consider the potential for financial loss and reputational risk resulting from policyholder fraud and claims fraud. Severe cases could potentially precipitate the economic ruin of insurers.

46. Policyholder fraud and claims fraud can be committed by policyholders at inception of the insurance contract, during the insurance contract or when claiming payment or compensation. Claims fraud can also be committed by third parties involved in the settlement of a claim. For example, medical practitioners could claim for medical services which have not been provided or engineers could inflate the costs of repairs.

47. The policyholder may deliberately withhold, or provide incorrect, background and other information, for example the refusal of coverage by other insurers or claims background. This is a serious risk for insurers, who might not have provided cover or who would have provided cover under different conditions (higher premium or higher retention) if they had been in possession of this information.

48. Examples of claims fraud are included in Appendix C – Cases of (alleged) policyholder fraud and claim fraud in insurance, and could have any of the following features:

- reporting and claiming of fictitious damage or loss
- exaggerating damages or loss covered by the insurance
- misrepresenting a fact to create the appearance of an incident being covered by the policy
- misrepresentation of the damaged party by an impostor
- staging the occurrence of incidents causing damage or loss covered under the policy.

49. Claims fraud could occur in combination with other types of fraud, such as identity fraud. There have, for example, been cases of medical treatment being given to people using the identity of others who are insured against the expenses of this medical treatment.

50. Insurers should deal with policyholder fraud and claims fraud risk as part of the operational risk of their business. In establishing the most appropriate policies, procedures and controls, insurers assess the benefits and costs of fraud prevention and detection, but need to:

- understand that while ease and speed of acceptance and claims settlement is desirable from a marketing perspective, it could result in a higher fraud risk. This risk may be mitigated by adequate anti-fraud policies, procedures and controls.
- consider their moral and ethical responsibility to prevent fraud and promote the integrity of the insurance industry.
- recognise that fraud affects their reputation – consumers may assume fraud is related to other criminal activities and expect that a high fraud frequency will lead to higher premiums or possible failure to pay claims.
- identify, prevent and detect types of fraud that should receive specific attention because they threaten the interests of policyholders or other third parties, for example, fraud by organised criminal gangs committing complex and extensive frauds and fraud for which other criminal action is needed, such as staged car accidents.[2]

4.2 Policyholder fraud and claims fraud deterring and prevention

51. Policyholder fraud and claims fraud deterring and prevention starts with adequate product development (product proofing [3]) by insurers. When designing a new insurance product, insurers need to be aware of risk enhancing factors. For example, policyholders in financial difficulties may be encouraged to stage the theft of a car or to commit arson to their property if the terms of the insurance contract provide for compensation on the basis of replacement value instead of current value or "new for old". This could be a consideration when deciding on the contractual terms of the policy. Insurers may also consider offering policies with claims replacement services. In these policies the loss is compensated by a replacement in kind instead of compensation in cash.

This is not to say that these terms should not be used, but insurers should be aware that they could increase the risk of fraud and should ensure appropriate controls to mitigate these risks are in place.

52. Insurers should assess the inherent fraud risk of their existing insurance products. In making their assessment insurers should involve those with relevant expertise, for example, fraud experts or claim settlers.

53. Insurers should establish an adequate client acceptance policy and consider for that purpose the following elements:

- Part of the client acceptance policy should include the categorisation of expected product-client combinations.

[2] Often the fraudulently obtained money is used to finance other criminal acts.

[3] The development of an insurance product in such a way that fraud risk and other

relevant risks are recognised and dealt with using adequate control measures

- For each combination it should be clear whether and under which conditions a client can be accepted and which measures insurers should take to prevent or detect fraud.
- The categorisation should be evaluated periodically. Part of this evaluation should include a comparison of detected fraud rates with expected fraud rates.

54. Insurers should establish adequate client acceptance procedures and consider for that purpose the following elements:

- Unexpected product-client combinations should receive special attention.
- Client should be identified and the identity verified.
- Approaches used for client acceptance include:
  - using professional judgement based on experience
  - checking red flag lists (Potential policyholder and claims fraud indicators – red flags are included in Appendix D)
  - conducting peer reviews
  - checking internal and/or external databases.

55. The procedures should include clear criteria that indicate which approaches should be used for each product-client combination. The effectiveness and efficiency of the client acceptance process and the success rate of fraud prevention may be increased by using automated means of checking client information against internal and/or external databases and against lists of red flags. This should be considered when deciding the extent of automation in the client acceptance processes.

56. Some insurers delegate their client verification and risk assessment processes to an intermediary. Nevertheless, they retain ultimate responsibility. As a result:

- Insurers should establish and implement a policy on client identification and verification and risk assessment by intermediaries.
- The terms of business with intermediaries should be consistent with this policy.
- Insurers should monitor compliance by the intermediaries with these terms of business.
- Insurers should have access to the identification and verification information concerning the risk assessment of clients.

57. Insurers should draw the attention of their policyholders and/or beneficiaries to their duties when taking out insurance or reporting a loss.

Examples include:

- minimising losses
- reporting claims in a timely manner
- co-operating in the investigation following a claim by providing insurers with all relevant information and, in particular, copies of official documents regarding the damage (accident, loss, etc.) in a timely manner
- authorising the insurers to carry out necessary inspections and to assess the extent of the damage prior to any repairs or replacement.

58. Insurers should inform both potential clients and existing clients about their anti-fraud policies.

59. Insurers should consider including in insurance contracts and in other relevant documents (for example, the claims form) provisions which make the policyholder, claimant and beneficiary aware of the consequences of submitting a false statement or incomplete statement. For example, they could be liable to prosecution or refused cover by the insurers. Where information is obtained orally (for example, in face to face meetings or telephone conversations) policyholders, claimants and/or beneficiaries should similarly be advised of the consequences of making a false or incomplete statement.

60. Insurers should consider the quality and reputation of third parties – such as medical practitioners, service engineers and contractors – used for compensation, restoration or repair of the loss or damage. Consideration should be given to using trusted third parties whose performance and business practices can be checked by the insurers.

4.3 Policyholder fraud and claims fraud detection

61. Insurers should be aware of the risk that the client might provide incorrect or incomplete information to obtain a lower premium or a higher coverage. Adequate policies, procedures and controls appropriate to the fraud risk profile of the product-client combination should be developed and implemented to detect incorrect and/or incomplete information when handling applications from new clients or from existing clients for new products. These policies, procedures and controls may include an assessment of the compatibility of the characteristics of the policyholder and the insured events.

62. Claim assessment procedures should be established by insurers. When handling claims, insurers should make an assessment of the fraud risk of the claim.

63. The procedures and controls for claim assessment may include :

- using professional judgement based on experience
- checking red flag lists
- conducting peer reviews
- checking internal and/or external databases or other sources
- using IT tools, such as voice stress analysis, data mining, neural networks and tools to verify the authenticity of documents
- interviewing claimants
- conducting special investigations.

64. The procedures and controls should include clear criteria that help the claim assessor to ascertain which assessment method should be used. The effectiveness and efficiency of the claim assessment process and the success rate of fraud detection may be increased by using automated means of checking claims

against internal and/or external databases and against lists of red flags. Insurers should consider this when deciding on the extent of automation in the claim assessment processes.

65. Insurers should consider that operational targets for efficiency of the client acceptance and the claim assessment processes may hamper fraud detection. Preferably, operational targets should be combined with targets for fraud detection.

66. Insurers that use claims adjusters or intermediaries for claim assessment will need to ascertain their competence and qualifications. Insurers may decide to limit the scope of action of claims adjusters and intermediaries (for example, by setting ceilings on the number or size of claims they can handle and/or the type of claims to be handled). Also, the fee structure for claims handling should not be set up in such a way that it diminishes the critical stance of the claims adjuster towards the (size of the) claim or loss.

67. Insurers should establish and maintain their own incident database. The database would contain the names of (former) policyholders, claimants, beneficiaries or third parties who could potentially attempt to defraud the insurers.

5 Intermediary fraud

5.1 Intermediary fraud risk

68. Insurance intermediaries – independent or otherwise – are important for distribution, underwriting and claims processing and settlement. It is possible for intermediaries to keep records of insurers' clients. Intermediaries are therefore involved in some of the most important processes and transactions of insurers and are crucial in insurers' operational and fraud risk management.

69. Intermediaries sit in a position of trust between the purchasers of insurance and insurers. Where trust forms a basic element of any transaction, there is the danger of this trust being abused.

70. Examples of involvement of intermediaries in fraud are provided in Appendix E – Specific cases and examples of (alleged) intermediary fraud in insurance, and include:

- withholding of premiums collected from a policyholder until a claim is reported
- insuring non-existent policyholders while paying a first premium, collecting commission and annulling the insurance by ceasing further premium payments
- colluding with policyholders to commit claims fraud or other types of fraud, for example, backdating transactions by providing false information to the insurer.

71. Typical warning signs [4] for intermediary fraud include where:

- the intermediary asks for payment of commission immediately or for payment of commission in advance
- the policyholder/insured lives outside the region where the intermediary operates
- an intermediary has a small portfolio but high insured amounts
- premiums received and commissions paid are above or below the industry norm for the type of policy
- the policyholder is asked to make payments via the intermediary where this is an unusual business practice
- the insured and the intermediary are represented by the same person
- there is a personal or other close relationship between the client and

the intermediary

- there are unexpected developments or results such as:
  - a high claim ratio
  - an increase of production that is exceptional or without apparent reason
  - a significant number of policy substitutions with complete commission
  - a high level of early cancellations or surrenders

4 The existence of these warning signs or indicators does not mean that intermediary fraud has occurred or will occur. Nevertheless, insurers should be looking out for these warning signs or indicators, particularly when more than one occurs.

- a high number of unsettled claims
- the portfolio of the intermediary has a (relatively) high number of insurance policies
  - for which the commission is higher than the first premium
  - with premium payments in arrears
  - with a payment shortly after inception (particularly life insurance) o with a high amount of claims fraud
  - with a disproportionate number of high risk insured persons, for example, elderly people
- the intermediary often changes address or name
- there are frequent changes in control or ownership of the intermediary
- there are a number of complaints or regulatory inquiries
- the intermediary is in financial distress
- the intermediary is involved in unauthorised third party business
- the intermediary appears to be churning policies
- the intermediary insists on using certain loss adjusters and/or contractors for repairs.

5.2 Intermediary fraud prevention and detection

72. Insurers should take all reasonable steps to confirm that the intermediaries they use meet fit and proper standards and have adequate safeguards for the sound conduct of business. In order to achieve this effectively, insurers should only grant terms of business to regulated intermediaries and should consider:

- having in place a documented policy and procedure for the appointment of new intermediaries
- having an application form and terms of business agreement that have to be completed and signed by the intermediaries
- ensuring the application form requires applicants to disclose relevant facts about themselves
- checking the financial soundness of the applicant and checking references
- having an effective sanction policy in case of non-compliance by the intermediary.

73. The terms of business agreements could require the applicant intermediary to

confirm:

- that the introduction of business to insurers pursuant to the agreement does not breach any other legal obligation or the rules of any competent authority in any relevant jurisdiction
- that at all times during the term of the agreement, the intermediary will maintain all obligatory licences, authorisations or registrations and comply with all applicable laws and regulations of the jurisdictions where it operates
- its compliance with the insurer's anti-fraud policies, procedures and controls.

74. In order to reduce the potential for commission fraud, insurers should consider:

- not paying commission before the first premium has been paid
- not paying more commission than a certain percentage of premiums paid
- keeping part of the earned commission in a temporary deposit when dealing with new, unknown intermediaries
- making a clear distinction between the funding of intermediaries and the payment of commission.

75. Insurers should have in place documented policies, procedures and controls to monitor the performance and business of the intermediaries. These policies, procedures and controls should be made known to the intermediaries. Elements to consider could include, but are not limited to:

- quality of business, including the soundness and ethics of the intermediaries' business conduct and integrity of their Boards, Senior Management and other staff
- anticipated and actual levels and patterns of business
- the warning signs mentioned in section 5.1.

76. Possible additional procedures and controls to prevent intermediary fraud for insurers to consider are to:

- send policies and renewal documents directly to the policyholders rather than via the intermediaries – intermediaries can be provided with copies
- instruct intermediaries not to accept premium payments in cash
- make all premium cheques payable to the insurer and not permit the intermediary to negotiate cheques payable to the insurer
- ensure that intermediaries operating client accounts have sufficient safeguards in place, with controls over who can operate the bank authorisations and with appropriate reporting lines
- have staff of the insurer or its auditor periodically audit the insurance business going through the intermediary.

6 Supporting organisational measures and procedures

6.1 Training of the Board, Senior Management and other staff

77. Insurers should organise initial and ongoing training on fraud matters for their Board, Senior Management and other staff. The type of training should correspond with the business process in which the person is engaged. Also, it should reflect the risks he or she may encounter in fulfilling his or her responsibilities.

78. At a minimum the Board, Senior Management and other staff should receive a general explanation of the insurer's anti-fraud policies, procedures and controls. This includes internal rules – for example, a code of conduct for the Board, Senior Management and other staff. They should be made aware of the need to report suspicions of fraud.

79. Some Board members, senior managers and other staff need, due to their assigned work, more specific training – for example, on relevant laws, anti-fraud policies, procedures and controls, fraud methods, trends and indicators, detection methods, and internal reporting procedures. In particular, fraud training should be provided to those who deal with:

- new business and the acceptance – either directly or via intermediaries – of new policyholders
- the collection of premiums
- settlements and payments of claims
- business with intermediaries
- recruitment of staff
- legal affairs
- internal auditing
- fraud risk management
- fraud investigations (for example, interview techniques and use of relevant IT).

6.2 Reporting suspicions of fraud

80. Insurers should have internal procedures requiring Board members, senior managers and other staff to report suspicions of fraud to a designated person[5]. Individuals reporting their suspicions of fraud in good faith should have adequate legal protection. In particular it is recommended that they not be held liable for disclosing confidential information.

81. Insurers should have a policy on keeping records of suspicions of fraud and fraud cases. This policy could provide for:

- criteria for the cases for which records should be kept
- the type of the information that should be recorded
- the period for which information should be kept
- access to the information, and
- safeguards for retaining the information securely.

82. Internal, policyholder, claims and intermediary fraud generate illegal proceeds. If an insurer suspects, or has reasonable grounds to suspect that the

proceeds of the fraud are
being laundered or are related to terrorist financing, its compliance officer [6] should report the suspicions promptly to the relevant competent authority which may be a law enforcement authority or a Financial Intelligence Unit (FIU).

83. Insurers should have clear policies for reporting suspicions of fraud to law enforcement agencies. How insurers choose to proceed will depend on the legal system and other characteristics of their jurisdiction, including any legal obligation to report criminal offences. It should be noted that a strict reporting policy by the insurer will contribute to countering fraud.

84. Insurers should communicate – internally and externally – their policies and procedures on reporting and sanctioning fraud.

85. Insurers should notify their supervisors of any fraud related matters which either require specific notification under the supervisor's regulations, or has been specifically requested by the supervisor. Insurers should at minimum report frauds with a (potentially) material impact on their financial position, business or reputation to their supervisors. Aggregate information about fraud and changes in fraud policies should be available to supervisors.

5 Depending on the type of fraud the designated person could be a director of the board, a (line) manager or a high level reporting officer, for example, a compliance officer or fraud risk manager.

6 In some jurisdictions the compliance officer is referred to as the money laundering reporting officer (MLRO).

6.3 Information exchange between insurers and other financial institutions

86. Fraudsters may target different insurers simultaneously or consecutively. Therefore, insurers should share information about fraudsters with each other. This may be achieved, within the limits of the privacy law and the data protection law of the insurer's jurisdiction, by timely communication between them and setting up shared databases.

87. A shared database may contain information about internal fraudsters and fraudulent policyholders, claimants, beneficiaries, intermediaries and other third parties.

88. Fraudsters may also target other financial institutions. Therefore, it is recommended that insurers, within the limits of the privacy law and the data protection law of the relevant jurisdictions, share information within the financial sector. This can be achieved by linking their shared database to databases operated by other financial institutions or setting up a shared database.

89. In addition to the exchange of specific information about fraudsters, insurers are recommended to share knowledge about fraud risk, trends, policy issues, prevention and detection. Cooperation with organisations involved with combating fraud in the insurance sector (such as organisations for chartered accountants, forensic auditors, claims adjustors, law enforcement agencies, supervisors and possibly consumer organisations) should be encouraged. This may include enhancing consumer/policyholder awareness on insurance fraud and its effects through education and media campaigns. Industry and trade associations can play an important role in this process.

Examples and cases of (alleged) internal fraud in insurance

Internal fraud includes a wide range of activities varying from straightforward theft, obtaining property by deception, data security breaches, breach of confidentiality and conspiracy, to attempts to obtain a pecuniary advantage by deception. Fraudulent and proper activities are often mixed and make the identification of internal fraud more difficult.

Theft or misuse of data for use in identity fraud and impersonation feature high on the list. Other types of internal fraud include:

- misappropriating funds
- fraudulent financial reporting
- stealing cheques
- overriding decline decisions so as to open accounts for family and friends
- inflating expense claims/over billing
- paying false (or inflated) invoices, either self-prepared or obtained through collusion with suppliers
- permitting special prices or privileges to customers, or granting business

to favoured suppliers, for kickbacks

- forging signatures
- removing money from customer accounts
- falsifying documents
- selling insurer's assets at below their true value in return for payment.

Some typical cases of internal fraud that have occurred or could occur within insurers include the following:

Case 1 – False employment history

An application for employment contains material falsehoods. The applicant claims to have just returned to the UK after a year travelling abroad. Investigation reveals that the employee was working in the UK during the previous 12 months and had been dismissed for fraud. Other examples could be the inclusion of qualifications not held, a false employment history, a false reference or the use of a false identity.

Case 2 – Falsification of claims

An insurer from the UK was defrauded by an employee for the amount of £ 1.5 million. This involved inflating the value of claims filed with the company and siphoning off the excess.

Case 3 – Theft of information

An employee reports witnessing another employee print confidential customer data and placing it in a bag. Investigation reveals that the employee had been offered money for the information while out for lunch one day in the company's uniform.

Case 4 – Intellectual Property Fraud; Computer Technician gets seven years in jail for stealing

Miss T. was a computer data entry technician for an insurer. She used her position to order the issuance of 42 claim drafts, for in total more than $207,000. These were subsequently mailed by computer from the insurer to T. at three separate addresses. She was arrested and charged.

Case 5 – Claims supervisor found guilty of theft

Mr S. was found guilty on theft for making fictitious claim payments to non-existent people. Mr S was creating claimants, manufacturing claims, authorizing payments and negotiating company drafts with the help of a niece, a teller at a local savings and loan association. Mr S. would call his niece each time he had worked the scheme to the point of draft issuance, and tell her the claimant would be in shortly, and ask her assistance in cashing the draft.

Case 6 – Office manager arrested

Mr P. was employed as office manager for an underwriting company. He was arrested and charged with the theft of $97,055, which should have been forwarded to an insurance company. The underwriting company was a general agent for the insurance company.

Appendix B – Potential internal fraud indicators – red flags

A red flag is an indicator that suggests the need for more detailed investigation of a fact, event, statement or claim. It may – especially in combination with the occurrence of other red flags – indicate potential fraud.

The existence of these warning signs or indicators does not mean that internal fraud has occurred or will occur. Nevertheless, insurers should be looking out for these warning signs or indicators, particularly when more than one occurs.

Business practices and condition

- Management turnover is high.
- Staff turnover in financial and accounting departments is high.
- Insufficient information is available about prior audits.
- The internal control structure is weak.
- Management operations and financial decisions are dominated by a single person or by several people who generally act together.
- Tasks and/or transactions are very complicated, requiring special skills.
- There are indications of financial trouble, for example, inadequate capital or increase in unpaid debts.
- Accounting principles are changed, revising an accounting estimate or a delay in issuance of financial reports prior to obtaining financing or another major event.
- Costs are rising unjustifiably or costs are substantially higher than costs from comparable business units or competitors.
- Training programmes are weak.
- The organisational structure is too complex.
- Internal audits do not exist or are weak.
- The Board has a very high proportion of executive directors.
- Members of the Board, Senior Management or other staff have external business interests and/or cosy relationships with contractors.
- Complaints or signals are received from external parties (like suppliers or

customers) and/or there are missing statements and unrecognised transactions.

- Security systems for data and assets are weak.
- Sudden changes are made to the insurer's strategy.
- Assets are restructured without explanation (for example, significant changes in non earning assets).
- Accounting is poor.
- Financial results and ratios do not correlate.
- Inexplicable changes in share value occur.
- Transactions, processes or expenses are poorly documented.
- Transactions are unusual as to time (for example, day of the week, season), frequency (too many, too few), place (too near, too far out), amount (too high, too low, too consistent, too different) and parties (related parties, strange relationships).

- Excessive credit adjustments (quantities and price) to a particular vendor occur and/or credit is issued by an unauthorized department.
- Procedural manuals for departments and/or divisions are lacking or not complied with.
- Board members, senior managers or other staff act in a dual role that leads to conflicts of interest (for example, acting as the internal auditor and claims manager).
- Unusual commission structure exists.
- Activities are not consistent with the insurer's stated policies.

Indicators in relation to (personal) conduct or attitude

- The Board or Senior Management place undue emphasis on meeting earning projections.
- Insurer's earning ability is lower than that of other comparable insurers.
- Insurer faces adverse legal conditions.
- The Board and Senior Management display a propensity to take undue risks.
- Members of the Board, senior managers or other staff have personal debts or financial losses incommensurate with their level of income.
- Members of the Board, senior managers or other staff appear to be living beyond their means.
- Board members, senior managers or other staff suddenly change their life styles.

- Board members, senior managers or other staff feel great pressure from family, peers or society or appear to undergo marked personality changes.
- Board members, senior managers or other staff believe that they are being treated unfairly (for example, passed over for promotion, refused pay rises or staff displacement).
- Board members, senior managers or other staff appear to exhibit extreme greed for personal gain.
- Fees for or expenses of the Board and/or Senior Management are high or have increased significantly.
- People suffer from a condition (for example, addiction to drugs, alcohol, gambling) causing possible financial debts or difficulties in controlling personal debts.
- Morale is low within the insurer or within certain departments of the insurer.
- Inappropriate relationships exist at work or people act in an unusual manner (for example, evasive behaviour, unexplained curiosity of people over financial controls, etc.).
- There are problems in recruiting staff.
- There have been instances of irregularities in prior years.
- The Board and/or Senior Management do not provide satisfactory answers to the supervisor's or auditor's questions or do not allow staff to speak to supervisors or auditors.
- The Board and/or Senior Management's reputation in the business community is poor.

- The Board and/or Senior Management display an overly aggressive attitude toward financial reporting.
- Management fails to follow proper policies and procedures in making accounting estimates.
- The Board and/or Senior Management place undue pressure on the auditor.
- The Board and/or Senior Management do not comply with laws and regulations.
- The Board and/or Senior Management display a dominant management style that discourages critical or challenging views from others such as staff.
- Managers or members of staff are working late, are reluctant to take vacations and seem to be under permanent stress.
- Payments are processed late in the day or after normal business hours.

- Payments are made in such a way that prescribed authorisation of others is avoided (for example, dual payments below the authorized payment level).
- Sales personnel provide coverage below market rates.
- Payments to third parties are made without appropriate supporting documentation.
- Insiders reduce their holdings of the insurer's stock.

Exaggerating damages or loss

Case 1 – Overcharge for damage repair

A report published by the California Bureau of Automotive Repair in 2002 indicated that of over 500 vehicles inspected after repairs, more than 40% of the bills included charges for work never done or for parts not used. The average overcharge was $586, (one-sixth of the average auto insurance claim after an accident).

Staging the occurrence of incidents

Case 2 – Staging car accidents by criminal gangs

Car accidents staged by criminal gangs are costing insurers millions of UK pounds each year.

In one example, a criminal group will arrange for a fee of £500 an accident for the fraudster, often at a roundabout, involving an innocent driver. One of the criminals will use the identity documents of the fraudster to impersonate him. The fraudster will subsequently file an insurance claim. The criminal group would also provide a fake medical report for a whiplash claim. Apparently, the average payout on a staged accident was £3,000, often with a £2,500 claim for whiplash damage.

In another example, a fake car crash could be staged for less than £2,000. Two drivable cars could be bought to stage a crash for £1,000. For an extra £800 a customer could buy £500 of comprehensive insurance, and another £300 of third party cover. After a fake crash had been staged all participants could claim £2,500 for whiplash injury and £5,000 for the written-off cars, fake car hire and loss of earnings. This way, fraudsters could collect on a £26,000 claim.

The Insurance Fraud Bureau estimates that it costs insurers between £48 million and £200 million a year. Apparently, the success rate for criminals is high since the police authorities do not have sufficient time to investigate.

Case 3 – Staging a car accident after illegal racing

A new car under comprehensive motor cover is used in illegal car racing, which

depreciates its value rapidly. The policyholder stages a car accident in the presence of independent witnesses. He would then claim compensation from the insurer for damage to his car.

Reporting and claiming of fictitious damage or loss

Case 4 – False mobile phone thefts

In Britain the police force receives 160 false reports of mobile phone thefts a month, which costs it £1 million a year to investigate. The National Mobile Phone Crime Unit estimates that between 15-20 per cent of mobile phone theft reports in the UK are false. Police suspect that false claims are sometimes encouraged by unscrupulous mobile phone shop staff looking for extra commission. Sometimes someone who has lost their phone will falsely report it as stolen in order to claim on their insurance. People think they're doing nothing wrong in lying to police and insurers.

Case 5 – faked theft of a cruiser

A man has been accused by police of staging the theft of his 39-foot yacht and was charged with insurance fraud, tampering or fabricating physical evidence, theft by deception and making false reports to law enforcement.

Authorities allege that T.L. faked the theft of his cruiser from a marina.

The boat was found later at the L. yacht club in E., Ohio. It was missing a flat-screen television, a cabin table, an anchor and a large piece of carpet, according to a criminal complaint.

Medical claims fraud

Case 6 – staged motor accident ring

An insurer in the US filed a lawsuit alleging that 67 chiropractors, doctors, medical corporations and individuals used a staged motor accident ring as a source of patients. The lawsuits claimed $14.1 million in restitution of paid claims and a further $42 million in damages.

Case 7 – claims for services not rendered

A 54-year-old man was charged with fraud and money laundering in connection with an investigation of a doctor who improperly prescribed painkillers.

G. W., a licensed chiropractor, was charged by the Pennsylvania Attorney General on Thursday for improperly billing the state Medicaid system for physical therapy sessions that were not supervised by a doctor or licensed physical therapist, according to the police

Mr. G. W. allegedly allowed patients to use a gym for “physical therapy” without assistance or direction from a licensed doctor. He billed the state Medicaid system, although law requires a direct supervision from a licensed physical

therapist or a doctor, according to the complaint.

A woman who was contracted to do medical billing for the office, became concerned when she noticed there was no supervision and no "blood pressure cuff, scale, stethoscope or medical waste box" at the L. office, according to the complaint. The woman refused to do medical billing until the physical therapy sessions were being properly supervised, according to the complaint.

Mr. G. W. is charged with nine felonies. He faces more than 20 years in jail and nearly $200,000 in fines

Case 8 – miscoding

The victim in this case is a US-based Fortune 500 company that operates a self-funded health care plan for its employees. The plan is administered by an outside health insurance company to which claims are submitted.

The fraud perpetrators include two individuals operating a health care clinic in California (as it happens these two individuals had "records" of securities fraud and for sexual misconduct with multiple patients, respectively). In addition to the above there were approximately six surgeons and laboratories involved in the fraud.

It first came to light when an employee reported that an unusually large number of employees were having cosmetic surgeries (not covered under the plan) performed at the expense of the company's health care plan. This was affected by miscoding, booking an operation as "the removal of painful scar tissue" when the operation performed was actually a "tummy tuck" or "liposuction".

Over the three years of fraudulent operation over US$ 1 million was paid out to the clinic.

Claims fraud related to money laundering

Case 9 – arson by a drug syndicate

A syndicate of drug barons bought a gold refining plant in Florida, insured with Lloyds', and burnt it down partly in order to launder "dirty" monies.

Claim related to terrorist financing

Case 10 – Insurance Policies to Support Terrorism

In 2004, students and brothers Yasser Abu S. and Ismail Abu S. were recruited to be members of a terrorist organization. Yasser Abu S. was apparently scheduled to perform a suicide bombing in Iraq. The suspects allegedly earned money through life insurance fraud to support international terrorism. Officials said they attempted to raise money by taking out an 800,000 Euro ($1 million) life insurance policy on Yasser, who intended to fake a fatal traffic accident and use the money for terrorist purposes. They were accused of 10 counts of fraud and 23 counts of attempted fraud.

Different types of fraud reported via a “cheat line’

Case 11 – Cheat line' turns tables on conmen

The Association of British Insurers (ABI), which set up a "cheat line", reported a sharp increase in the number of people reporting false insurance claims and indicated that these reports have saved insurers millions of pounds. One insurer estimates that it has saved £1.5 million as a result of information received from the hotline.

A third of calls relate to household insurance, mainly fictitious burglaries or deliberate fires. Another third involve car accidents. Some 17 per cent concern bogus personal accident claims, with one in 10 callers informing on companies making dubious commercial claims.

In one case a £60,000 claim for a written-off Ferrari was rejected when someone reported that the accident had happened at a rallying event.

Fraud by a third party involved in the settlement of the claim

Case 12 – Independent adjuster arrested in shakedown scheme

Mr. B., an independent adjuster, was hired by an insurer to conduct an inventory at a retail department store, after the store had been burglarised. The owner of the store, who cooperated with the investigation, had reported a loss of $33,599 to his insurer. The investigators electronically monitored conversations between the owner and Mr. B, wherein Mr. B. stated that he had figured the loss to be much lower than reported, but offered to “inflate’ his inventory in return for 7%. B. agreed to a cash payment of $2,000. When Mr. B. was overheard accepting the payment from the owner, he was placed under arrest.

Appendix D – Potential policyholder and claims fraud indicators – red flags

A red flag is an indicator that suggests the need for more detailed investigation of a fact, event, statement or claim. It may – especially in combination with the occurrence of other red flags – indicate potential fraud.

The existence of these warning signs or indicators does not mean that fraud has occurred or will occur. Nevertheless, insurers should be looking out for these warning signs or indicators, particularly when more than one occurs.

General

Claimant’s behaviour

- The claimant is aggressive when applying for a policy. When making a claim he/she is very demanding and/or insists for quick settlement.
- The claimant enquires frequently about the progress of the claim handling.
- The claimant threatens to bring in a lawyer if the claim is not settled

swiftly.

- The claimant wants cash.
- To deal with the claim quickly, the claimant is willing to accept an inexplicably low settlement.
- The claimant did nothing to prevent or limit the damage.
- The claimant is unwilling to co-operate during a reconstruction and/or gives evasive answers.
- The claimant handles all business in person or by phone, avoiding written communication.
- The claimant does not want other people, for example, family, friends and neighbours, to know what happened.
- The claimant gives inconsistent statements to the police, experts and third parties.
- The insured has detailed knowledge about insurance terms and the claim process.
- The insured has checked the insurance coverage shortly before the claimed event.
- The policyholder has several policies with the same insured object and coverage.
- The insured requests that payment is made into different accounts.
- The insured changes address, bank or telephone details shortly before a claim is made.
- The claimant request payment to be made to a third party.
- The claimant insists without proper reason on using certain contractors, engineers or medical practitioners or wants to use relatives.
- The way a claim is filed is remarkable (for example, the claimant used a lawyer or sought professional advice in claims reporting).
- The policyholder changes insurer frequently.
- The policyholder has been denied insurance before and has not mentioned this when applying for insurance.
- The policyholder insists on changing terms and conditions.

Documents

- The claimant is not able to provide documentary evidence for major losses, such as receipts or photographs (and minor losses are documented).
- Documents, for example, receipts, are not specific or the name of the

buyer is filled in later. Documents are changed or are unreadable.

- Original documents/receipts are missing, only copies are provided.
- New receipts (not wrinkled, very clean) are provided for old events or products.
- There is different handwriting on various receipts.
- The dates on documents are strange (for example, in relation to holidays, business hours etc.).
- Receipts are provided from companies that do not exist, have ceased operating or are insolvent.
- Receipts with differing dates have successive numbering.
- The currency on foreign receipts is not specified.
- A “pro forma” receipt is provided.
- The application form is not completely filled in and/or not signed.
- The claim form is not completely filled in and/or not signed.
- Alterations are made in the claims form to create appearance of cover.
- There is a big difference between the receiving date of the application form and the inception date of the cover.
- There are inconsistencies between the application form and the claim form.
- There are variations in or additions to the policyholder’s initial claims.
- Supporting documentation is supplied by parties related to the insured or claimant.
- Reports from medical practitioners or others (for example, police authorities) are inconsistent.
- Documentation from foreign countries deviates from the expected format or contents (for example, use of incorrect language).

Characteristics of losses

- The claim is filed either shortly after coverage becomes effective, or just before cover ceases or shortly after the cover has been increased or the contract provisions are changed.
- The loss occurs just after payment of premiums that were long overdue.
- Damage has occurred in the period of provisional cover.
- The loss was not reported abroad where it occurred.
- There are inconsistencies between the insured amounts and the characteristics (for example, age, profession) or life style of the insured.
- Actual loss is far higher than first reported loss.

- Claimed loss is just below a threshold that causes additional checks by the insurer.
- The insured interest is questionable.

Characteristics of claimant

- The insured's financial situation is bad.
- The insured lives in a known fraud area.
- The policyholder or claimant has a relationship to known fraudsters or criminals.
- The insured's family situation is difficult (for example, recently divorced).
- The insured's occupational situation is unusual and/or difficult (for example, he/she is unemployed or self-employed, frustrated with the job, facing disciplinary action and/or revocation of professional licensing, a seasonal worker where the active labour season is coming to close, or employed in an industry or company that is experiencing lay-offs or downsizing).
- The claimant uses a post office box or hotel as his/her address, has moved a lot, gives a false address, or his/her telephone number does not match the address.
- The policyholder is the partner of the claimant.
- The claimant has a bad claims history.
- There is a certain connection between the claims.
- The identity of the policyholder, the insured or beneficiary cannot be determined.
- The insured frequently makes high claims.
- The insured will not disclose his claims history (with other insurers).
- The claimant insists the payment should exceed the value of the damaged goods.
- Claims are submitted by a third party without proper power of attorney.
- The claimant cannot be contacted through normal channels.

Property claims (including disaster fraud)

A major disaster provides an ideal opportunity for fraudsters. Insurer's resources are stretched due to the large number of claims, so that they are not able to evaluate claims as thoroughly as they normally would.

- Losses fit in badly with the insured's characteristics, such as residence, occupation, income and/or lifestyle.

- A large amount of cash has been stolen.
- According to the claimant, the insured claims items were new.
- The claimed items are (substantially) over-insured.
- No police report is provided in cases where you would expect one.
- The insured is unable to describe the losses adequately.
- At the preliminary stages of the claim, the insured gives a very detailed description of the property or has a detailed photo report.
- The damaged items are not/cannot be examined by the loss adjuster.
- There are unexplainable differences between the claimed losses and the findings in the police report.
- The insured's items were up for sale.
- An insured company has expansion plans.

- The insured items were in bad shape.
- The order of the list of property provided by the claimant is exactly the same as in the loss adjuster/claim inspector's report.
- During a fire or other disaster neighbouring buildings were not affected.
- Coincidental absence of the insured, family or pet at the time of a fire is suspicious.
- Detailed investigation makes it clear that no sentimental items (such as photograph albums) or family heirlooms were lost or damaged.
- Characteristics of the losses are incompatible with the season in which the losses are claimed.
- There is no physical evidence of the place where heavy items were located (like indentations in the carpet from furniture).
- More than one source of fire is found.
- The origin of the fire is unknown or conspicuous/suspicious.
- In case of arson there is no evidence of burglary.
- At the time of the fire the building was unoccupied and without surveillance.
- At the time of the fire the building was not connected to public utilities.
- The fire was not detected by the fire alarm.
- The fire alarm was "coincidently" switched off.
- The fire alarm was switched on, but "blocked" by objects.
- The fire is detected shortly after people have left the building.

- Vehicle theft and casualty/damage
- These types of fraud normally occur when the claimant exaggerates the car damage and/or his injuries, totally fabricates claims or stages an accident.
- The claim involves victims with no own damage insurance and/or one who would be at risk if found at fault.
- One of the people concerned reports a suspicion of a set-up.
- The insured was involved in accidents before, with similar circumstances and/or with the same lawyer.
- The insured (too) easily agrees to accept the blame.
- There are inconsistencies in the claimant's account (for example, who was driving and what the final destination was).
- After an accident with substantial damage, the police and/or emergency services were not called.
- After an accident with substantial damage, a claim for recovery damage was not made.
- The passengers of one of the vehicles involved did not have personal relationships with each other.
- There is a relationship between the people involved (for example, between passengers of the different vehicles or between passengers and doctor).
- One of the people involved has a rental car.
- The driver of the rental car accepts blame easily.
- The witness is very co-operative.
- An old car bumps into a new car.
- Severe damage is incurred without a collision (for example, swerving).
- Both people involved are foreigners from the same country.
- There are several very similar testimonies or striking differences between the testimonies.
- There are remarkable similarities in the reported injuries, the medical reports or the repair shops or doctors involved.
- The damage does not match the injuries (for example, little physical damage but severe personal injuries).
- There are inconsistencies in the damage of the involved cars (one with minor damages, the other with severe damages).
- The injuries, such as headaches or whiplash, cannot be objectively observed.
- There are no marks at the location of the accident.

- The accident took place at a deserted location.
- The claimant's employment information is suspicious.
- The claimant started his employment shortly before the accident occurred.
- There was a delay in filing the accident claim.
- The date of modification is too close to date of accident.
- The claimant does not want the claim handler to contact his employer directly.
- The car has an unusual registration number.
- The registration number had just been registered.
- The car is stolen just after the end of the "new-value period'.
- The car theft took place where parts of the registration certificate were in the car or were lost before the theft.
- The car keys are not the original ones.
- There is an unclear story about the use of the key.
- The alarm was switched on but did not work.
- The stolen car is recovered completely undamaged (or locks are not damaged).
- The stolen car is recovered with valuables/documents.
- There is inconsistency between the age or social position of the insured and the type of the car.

Travel

- The insurance term does not match the holiday period.
- Insurance is only bought for the days of journey, not for the stay.
- There is inconsistency between the loss and the living standard or the amount of luggage of the claimant.
- The loss is reported a long time after the trip.

Life

- The insured dies abroad.
- The body of the deceased is not found or identified.
- The (original) death certificate is not available.
- The cause of death or disability is suspicious.
- A claim of suicide or a criminal offence arises shortly after inception of the policy.
- Policy provisions or beneficiary are changed just before death or

disability.

- Payments are requested to be made to others rather than the policyholder, the insured or the beneficiary.
- The premium is paid in cash.
- The premium is paid in foreign currencies or from a foreign bank account.
- There is inconsistency between insured amount and standard of living of the insured.
- There is a large age difference between insured and beneficiary.
- The policy is cancelled or a refund of premiums is requested shortly after the cooling-off period.
- The application is just below the limit that would trigger a more detailed examination of the application.
- A disability claim arises just after a premium default.
- The relationship between the policyholder, the insured and the payer of the premiums is unclear.
- One policyholder or beneficiary has several policies with different address data.
- The policyholder accepts unfavourable conditions.
- A request for cancellation is not signed or is signed by an unauthorised person.
- There is an inconsistency between the beneficiary's name and account number.
- Early surrender or encashment of the policy especially if against unfavourable conditions (for example, loss of tax benefits or deduction for expenses made by the insurer).
- The beneficiaries are changed frequently.
- Payments are made to unrelated third parties.

Transport

- A high quantity of goods is stolen given the available time frame.
- Packed goods are repacked to larger volume entities, for example, pallets.
- The endorser is different from claimant.
- Transportation is to final destination that does not have a market or proper processing facilities.
- There are gaps in the dossier.
- Goods to be transported to developing countries are overvalued.
- Intermediaries do not cooperate.

- The tachometer is damaged or missing.
- The parties in the transport sector have bad reputations.
- The weighbridge is not calibrated.
- There are inconsistencies between the insured amount and market prices.
- There are inconsistencies between the insured volume/weight and the real weight.
- There are inconsistencies between the insured volume/weight and the type of goods.
- Goods are delivered (at a later date) after theft.
- The drivers are paid per trip.
- The policyholder is different from the applicant for provisional cover.
- Documents are put ready in hotels or restaurants without sufficient supervision.

Healthcare

- Improper identification numbers are used.
- The diagnosis is incorrect or the adjuster receives conflicting medical opinions from medical providers.
- There was no communication with emergency services.
- Prescriptions are cut or have been altered.
- The claimant has multiple disability policies.
- The treatment being provided to the claimant is inconsistent with the report diagnosis.
- The claimant is involved in active employment or in a physical sport or hobby although he claims his disability prevents him from engaging in sedentary work.
- Treatment dates appear on holidays or other days that medical facilities would not normally see patients.
- The claimant later develops additional injuries allegedly related to the initial injury or illness when it appears the claim will be terminated.
- Medical terminology on the documents is misspelled or misused.
- The claimant changes attending physicians frequently.
- The attending physician is not in the same geographic region as the claimant.
- The attending physician’s specialty is not consistent with the diagnosis.
- The claimant’s illness or injury occurs shortly before an employment problem (for example, disciplinary action, demotion, layoff, strike,

termination, or down sizing).

Appendix E – Specific cases and examples of (alleged) intermediary fraud in insurance

The most common example of intermediary fraud is where an intermediary takes the premium from the purchaser and does not pass it to the insurer resulting in no insurance cover being in force (premium diversion). This can go on year after year, especially where the intermediary has delegated powers, with the policyholder not becoming aware of the situation until a claim is made.

A variation of this is where an intermediary inflates the premium, passing on the correct amount to the insurer and keeping the difference as well as earning any commission due on the transaction.

Another example is non-disclosure or misrepresentation of the risk to reduce premiums in order to win the business. Again the policyholder only discovers this when a claim is made which can be years later.

These frauds can have subtle variations:

- Alleged cover does not exist as the premiums have been stolen by the intermediary and not passed on to the purported insurer. The result is the purported insured loses his/her money.
- Alleged cover does exist but the premiums have been stolen by an intermediary who has binding authority. The result in this case is the purported insured would be covered due to ostensible authority issues but the insurer loses out as it has to provide cover for which no premium has been received.
- Alleged cover does not exist with the purported insurer or has been placed with a sub-standard or fraudulent insurer. Policyholders are then not covered by the insurer named in the policy documentation and claims may not be met by the actual insurer.
- Alleged cover does not exist and the intermediary intends to act as insurer and pay claims. The result would be that some insured persons would have their claims paid and some may not. As intermediary runs out of premium to pay the claims, the tendency is to seek more and more policyholders to cover the losses. When the scheme finally collapses there are a large number of victims.

Commission fraud by an intermediary occurs when insuring non- existent policyholders while paying a first premium to the insurer, collecting commission and annulling the insurance by ceasing further premium payments.

Also, intermediaries might collect commission from the insurers and at the same time charge the insured a consulting fee (in some jurisdictions this would be illegal).

Case 1 – Commissions and "bid rigging"

A civil complaint was filed by the New York Attorney General against M. The allegation was that for years M. received payments from insurers that were in addition to upfront sales commissions, so-called "contingent commissions" and that fake bids or quotes were solicited, which may not have been competitive.

The complaint refers to internal communications in which executives discuss how to maximise M.'s revenue and insurers' revenues (without regard to the clients' interest). An example of such a communication was allegedly the message: "We need to place our business in 2004 with those (insurers) that have superior financials, broad coverage and pay us the most".

Major insurers were named as participants in steering and bid rigging.

According to the complaint, M. collected approximately $800 million in contingent commissions in 2003. The civil complaint tries to end the steering and bid rigging.

In January 2005, M. reached a settlement agreement with New York. As a result, the company enacted reforms to address the complaint. Under the terms of the agreement, M. neither admitted or nor denied the allegations in the complaint. M. agreed to forgo contingent compensation and to disclose all forms of compensation received from insurers. Also, M. will provide all quotes and terms received from insurance carriers and adopt a compliance and conduct policy for the firm. A fund also was created to compensate clients. However, the fund did not represent a fine or penalty.

The investigation implies that the mere existence of contingent commissions leads to the misconduct. However, many independent insurance agents and brokers in the U.S. receive contingent commissions for placing quality business with carriers without allegations of misconduct. Under the terms of the settlement, M. was not fined or penalized for receiving contingent commissions.

It is important to note that no regulator or government official has ever said or found that contingent commissions are per se illegal or impermissible. In fact, in all of his carrier settlements, carriers are expressly permitted to continue to make such payments. In addition, none of the actual claims in the complaint turn on the payment of contingent commissions.

Case 2 – Fictitious valuations

Another example concerns one of the principals of an intermediary firm who deliberately provided wrong information regarding the value of policies to clients.

This individual had been providing investment services from 1997 to two particular structures on behalf of two American business partners. The portfolios held approximately $3.5 million and $3 million at the outset. The clients and USA advisors had sought target growth of 12 – 15% p.a. They stipulated that they

would require fixed annuity payments from the companies of approximately $300 thousand each. There is a further structure that has also been administered by the intermediary which had an initial investment of approximately $600 thousand.

The intermediary managed to achieve the required growth for the main portfolios in the first year but failed to reach the targets from about 1999. Instead of reporting this to the clients he falsified the valuations in the hope that the portfolios would bounce back. The investments not only failed to reach targets but actually fell in value. The capital was being eroded further by the annuity payments continuing to be maintained. He continued to provide the false valuations over a period of years until he ran out of investments with which to pay the clients' annuities in January 2004. At this point he reported the matter to his legal advisers, who in turn advised him to report it to the supervisor.

By his own admission, he had been providing false investment statements over a prolonged period of time. He did not take the opportunity of coming clean until it was clear that the cover up could not continue. Although he claims not to have profited out of the manipulation of the investment portfolios, the fact that the intermediary charged a fee of 0.5% of their (false) value means that he has benefited indirectly.

There was no supervision of the adviser, who kept the client file locked away and did not allow any administrative staff or the other principal of the business to handle the file according to procedure.

Case 3 – Backdated cover

An investigation into a firm was carried out where allegedly the intermediary was backdating motor insurance policies to give motorists the appearance of insurance coverage after an accident had already occurred. In exchange for this illegal activity, the agent/broker

demanded a fee. In this case some applicants were charged up to $3,000 for a backdated policy. Numerous claims were investigated from three affected insurers.

Case 4 – A bogus insurance programme

An intermediary based in the US collected $3.8 million in a nationwide bogus insurance programme. The intermediary was arrested and charged on 63 counts relating to the sale of thousands of fake insurance policies throughout the US.

Case 5 – Fraud against a reinsurer

In this case the premium for reinsurance was far less than the ceding insurer knew it would have to pay out as claims.

The fraud occurred in the reinsurance market of the personal accident element of US Workers' Compensation business. The market was found to comprise a handful of players, based primarily in London and Bermuda, who were prepared

to write what they knew to be gross loss making business relying on their reinsurance to make net profit. This kind of underwriting involves no real assessment of the risk and has been referred to as arbitrage" or "net underwriting". The judge described the market as being like a game of pass the parcel" and as being economically unsustainable as each player passed certain losses on to his reinsurers who did the same to their reinsurers. Characteristic of the market is the creation of spirals as losses, rather than being dissipated by outwards reinsurances, are concentrated on certain insurers higher up the chain. Inevitably, the market ended in disaster and the losses sustained in relation to this action alone stand at $250 million and rising. The court held that a market that traded in losses of this type was one in which no rational and honest person would have participated if he had understood the market and proper disclosure had been made. Documentary evidence showed that the true nature of the business was deliberately and fraudulently concealed.

Involvement of the underwriter

S. had granted a binding authority to their underwriting agent E. at a time when E. had already been in discussion with the brokers S. about using the binding authority to write Workers Compensation carve out business. It was found that when S. granted the binder to E., the nature of the business which the E. underwriters intended to write was fraudulently misrepresented to S. and that at no time was S. told the true nature of the business being written by E. Of 119 contracts written under the binder, 112 of them were broked by S. Those 112 contracts generated premiums of $25 million but the losses amounted to in excess of $250 million. The E. underwriter confirmed in his evidence that he wrote the contracts in the expectation that he would be able to recover most of the losses from reinsurers.

Involvement of the broker

It was also found that S. knew that E.'s acceptance of the programs was dishonest and in breach of E.'s duties under the binding authority, and that S. had therefore dishonestly assisted E. in breaching those duties. The judge described the actions of S. and E. as: "a chronicle of deception that induced insurers to become involved in a business in which they would have never have been involved if the business had been properly explained to them".

Involvement of the reinsurer

However, whilst the judge found no dishonest conduct on the part of anyone at S., he did find that the conduct of the underwriter at S. responsible for agreeing and supervising the binding authority had: "fallen well below that which was to be expected of any competent underwriter; if he had not acted with such gross negligence and dereliction of duty (which S.'s internal controls failed to prevent), the dishonesty of E. and S. would have been investigated long before it was". S.'s holding company was considering an appeal: "To characterise S. as a

victim in this is preposterous. They were part of the market; they knew what was going on. I think the judge saw himself charging in on a white horse and took offence to the way this slightly wacky world of reinsurance operates".

Case 6 – Agency owners sentenced for theft

Mr W. and Mr C. were co -owners of an agency company. It appeared that $277,004 premium, paid to the agency by a School Board, had never reached the insurer. The School Board's premium was for fleet and multi- peril coverage. After being notified of a rate increase, the School Board decided to reject the offer and advertise for new bids. The insurer then notified the School Board that its premium of $197,532 was past due. Investigation determined that the $270,004 cheque from the School Board had been deposited into a money market account of Mr W's agency company. The bank records were subpoenaed; the records were obtained; the money was gone! Where the money had gone, was unimportant. Where it not had gone (the insurer) formed the basis for the charge of theft. A detailed audit turned up some other cheques he "forgot" to forward to the company.

Case 7 – Premium for $22,000,000 in insurance for hotels

Mr L, an insurance intermediary, accepted a premium of $408,570 to place $ 22,000,000 in property and liability insurance for a hotel group. One cheque was issued for the entire premium, on behalf of the six hotels. Mr L. deposited this cheque into his account and used approximately $77,000 of it to buy some insurance for the hotels. Unfortunately for the hotels, Mr L. had a lot of personal debts. He used the "change" (about $170,000) to buy himself a boat and a condo. L. admitted manufacturing and altering several documents to indicate the proper amount of coverage for the premium paid by the hotel group.

2013

Indian helicopter bribery scandal

The UPA government initially denied all allegations and claimed it has "nothing to hide" and that "our track record is not cover up"[

A complaint has been filed seeking an investigation into the sale of 21 civil helicopters worth over Rs 7,000 crore (US$1.6 billion) by AgustaWestland between 2005-2013 in India. As per the complaint Agusta Westland has been selling civil

helicopters in India through its agent Sharp Ocean Investments Limited, which is promoted by twin brothers Nayan Jagjivan and Nakul Jagjivan. Tax authorities in India have been asked to probe the possibility of tax evasion by Sharp Ocean on the commission received for the sale of helicopters and foreign exchange deprivation to the country by off-shoring payments for the sale of helicopters in India.

Separately, the Comptroller and Auditor General, in its latest report, has indicted the Chhattisgarh government for overpaying Rs.65 lakh (US$120,000) for the purchase of a VVIP chopper -an Agusta A-109 Power helicopter from Sharp Ocean Investment Ltd and its India representative, OSS Air Management. Both companies are promoted by twin brothers Nayan Jagjivan and Nakul Jagjivan.

Cancellation of the contract by the Indian Government

India cancelled the ₹3,600 crore deal within January 2014. The government cancelled the contract "on grounds of breach of the Pre-contract Integrity Pact and the agreement by AWIL (AgustaWestland International Ltd)". The contract was frozen in February 2013 after allegations surfaced that Rs 360 crore was paid as bribe.

Role of Union Law Ministry and Indian President in CBI probe

Recovery of Bank Guarantee

After the cancellation of the contract, India encashed over 250 crore made by AgustaWestland as bank guarantee in the Indian banks in January 2014. Separately, India requested the Italian government to retrieve the bank guarantee amount made by the firm in Italian banks which was more than €275 million (2364 crore). On 17 March 2014, request made by India was rejected by an Italian court. However, the appellate court, Milan reversed the lower court's judgement and upheld the claims of the Indian government. Accordingly, in June 2014, Indian government encashed 1818 taking the total amount recovered so far to 2068. With this, India has recovered the entire amount of around 1620 (45% of total contract value 3600 crore) it had paid to AgustaWestland.

Now we come for the last session of the day,what aconomic crime impact is on energies utilities and mining. And without any preliminary or anythig May I just Request Mr. Justice Gowda to enlighten us on energies utilities and Mining. It will be a treat to listen to him.

My very affectionate brother U U Lalit and my brother and Sister Judges, Director, Research associates of this institution and staff of the National Judicial Academy. I thank the academy for this topic which is of great concern today and in recent years. The constitutional mandate provides for preservation of energies utilities and mining. natural resource is very important to achieve constitutional goal of eqality in India. SC in 1973 in Keshvanada Bharti case before 44th amendmend has to deal with land reform bill and power of parliament to amend will. It was looked by 13 judges.Part III and IV was human rights. Federal feature of the constitution,vast geographical areas and States were required to govern the people keeping in view constituional mandate. Keeping this in mind I will deal with topic with idea of good governance.

Countering fraud and corruption in minerals and mining.The international minerals and mining sector faces many challenges – operating in remote territories and in jurisdictions and cultures that are very different from those in the country where the parent company's headquarters are based, facing pressures on commodity prices in a volatile global economy that results in tight margins, and ever increasing production costs. Companies go some way to protect themselves against breaches of global corruption legislation (such as the US Foreign Corrupt Practices
Act and the UK's Bribery Act) but very few take action to reduce the real cost of fraud. Fraud and corruption present a real risk to the industry and mining security and audit professionals, when faced with a financial crime investigation, need to take positive, ethical and effective action. Working with the University of Portsmouth's Centre for Counter Fraud Studies, PKF Littlejohn has developed a course to equip delegates with a range of skills and knowledge to enable them to not only investigate allegations of fraud and corruption, but also to undertake action to better protect their organisation from these crimes. DeliveryThe course will be delivered by a mix of distance-learning and attendance at a one-week event at a conveniently located venue.The distance-learning elements will be available to delegates online, enabling them to be accessed at any time of day in orderto suit the delegate's own needs. The material will be a mix of PDF, audio, video and web resources, backed-up by tutor support via e-mail. The distance learning will then be consolidated by attending a one-week event in the delegate's own region. Tuition will be delivered by a mix of Accredited Counter Fraud Trainers and subject experts and will include practical exercises to enable delegates to apply their new-found knowledge and skills in a

learning environment.As well as developing knowledge and practical skills, the event will allow delegates to network with colleagues from across their region in a collaborative environment. Assessment Delegates will be required to complete a number of assignments during the distance-learning stage of the course; following completion of the residential stage, delegates will then be required to complete one final written assignment. Successful completion of the course will lead to the award of the Accredited Counter Fraud and Counter Corruption (International) Practitioner qualification from the UK's Counter Fraud Professional Accreditation Board. Delegates will also receive a certificate from the University of Portsmouth confirming the award of Higher Education credits which can be used to gain entry to further course. The recovery in metal prices has encouraged mining and metals companies to reactivate capital projects and exploration activities. Often in the quest for expanded production and higher returns, these projects are being conducted in countries more prone to corruption, and hence greater risk. Cost reductions from the financial crisis have created slimmed-down control environments, which only put companies at greater risk.

Recognizing this situation, those most responsible for governance of the organization (e.g., the board of directors) are searching for risk mitigation strategies that also contribute to their corporate sustainability efforts. Draw upon our experience "at the coalface" to:

- Update your understanding of the rapidly changing fraud and corruption risk environment
- Make a high level assessment of your company's changing exposure
- Create a roadmap that combats fraudulent and corrupt practices.

Highly publicized press over alleged fraud and corruption in the sector — a major iron ore producer in China, a global diversified in Cambodia and a global copper and gold producer in the Democratic Republic of Congo — has only increased the notion that the sector is an easy target for fraud and corruption. Certain characteristics predispose miners to fraud and corruption risks, including:

- Labor-intense operations
- High-value commodities
- Dependency on local communities
- Highly regulated activities
- Largest source of local economic activity
- Large royalty and tax takes
- Remoteness of operations

- Operating in countries with endemic corruption
- The requirement for large capital investments
- Environmental impact
- Frequency of merger and acquisition activity

Fraud and corruption are typically covert events that can go undetected for years, or altogether. This is because the people committing these acts understand the weaknesses either in the processes or systems, and exploit them. They also improve their skills as they continue to perpetuate these activities, effectively learning on the job, making them harder to detect. Whether one is referring to a lapse in safety standards, a bribe paid overseas to retain an existing contract, or a senior executive acting for personal gain, the speed of the reaction of regulators, law enforcement and the financial markets can quickly overwhelm management and boards of directors alike. Without tackling corruption risk effectively, your company can face irreparable damage. Some elements include:

- Your social license to operate
- The ability to access new projects
- The return of value to shareholders
- The reputation of the organization

Management of potential fraud and corruption in the mining and metals sector is critical for the following reasons:

- Provides tangible evidence of a culture of integrity
- Helps to minimize fraud and facilitates early detection
- Limits unpleasant surprises that can distract management
- Addresses concerns of external auditor and board of directors
- Limits potential for class action lawsuits
- Safeguards the assets and reputation of the company on behalf of investors

Ultimately, fraud and corruption risk is related to corporate governance, business ethics and crisis management. And like crisis management, the time to develop your plans and procedures is not when the world is at your door looking for answers. Addressing the need for ethical business conduct and how your organization will deal with any lapses is of paramount importance. These plans and procedures need to be developed through an understanding of how fraud and corruption is committed and the personal and business indicators of that behavior.

As the people involved in the commission of these types of offenses do not want to get caught, and want to keep what they have taken, they will exploit their knowledge

of your controls and processes to continue to commit their crimes.To combat this, it is necessary to increase the perception and reality of detection through clever tactics and solutions, aimed at preventing and detecting.

The Odisha illegal mining scam amounts to Rs. 59,203 crore and illegal iron and manganese ore amounting to 22.80 crore tonnes was extracted illegally from the state for almost a decade, the Shah Commission report has said. It has demanded a CBI investigation into the matter, warning that too many powerful people, businessmen from Odisha and outside the state, bureaucrats and politicians are involved. The Hindu accessed more parts and contents of the report which the government has classified as secret and asked the Supreme Court not to put out. The paper had earlier also reported on the gross violations of laws recorded by the commission. The report notes that the state police and other state authorities, which suddenly filed cases when the inquiry by Shah Commission became imminent, are incapable of carrying out a thorough probe and catching the powerful but guilty parties. It suggests that these cases have been filed only as a cover to deny the CBI inquiry. The state is unable to prosecute anyone, the Commission has said, "Since there is involvement of mighty lessees, big traders of the state and from outside the state, political entities and officers of higher ranks. It will not be possible for state police to find facts and realities and there would be no justice for the quantum of illegalities that took place."

It has demanded a CBI inquiry not only in to the illegal mining, but also the attendant railway freight scam and linked evasion of excise duty by the mining companies. It is one of the most scathing reports to come out of the stable of Justice M.B. Shah Commission on illegal iron and manganese ore mining as yet and it holds businessmen, state government and the centre, all responsible for the systematic exploitation of natural resources and linked rampant corruption. The report says, "All modes of illegal mining a are being committed in the state of Odisha. There is a complete disregard and contempt for law and lawful authorities on the part of many among emerging breed of entrepreneurs, taking undue advantage of country's natural non renewable assets and resources for export earnings." It adds, "The pursuit of super profits has absolutely drained them of any feeling for fellow human beings/for nation and the moral values. The law has been made helpless because of its systematic non implementation."

The Shah Commission goes on to list each company that mined thousands of crores of ore in blatant disregard of all mining and environmental laws. In some cases it notes that mines ran illegally for more than two decades. "The Hindu had earlier reported the gross violation of environmental laws elaborated in the report. The parts

of the report accessed by the paper now also detail the rampant and wide-ranging violation of mining regulations. The report states, “Amendment to mining lease is permitted only for conservation of minerals, protection of environment or safety. In 85 mining leases IBM has modified the mining plan. In 30 cases there were modified two or more times. In 53 mining leases IBM approved amendments retrospectively. In 49 it was amended for increase in production. In these 49, from the year 2000 till date production was permitted to increase from 41.634 million tonnes to 118.978 million tonnes. In 8 cases the production limit was increased from 18.940 million tonnes to 49.080 million tonnes. At this rate all the iron ore reserves in the state would be exhausted in 30 years.” The miners have made a killing out of the illegal exploitation of natural resources, the Commission writes. For example it shows how the government-owned NMDC showed its costs as only 16% of the annual turnover but another private company during the same time showed 62.38% cost for mining only to substantially reduced its profits on records.

Warning that the super profits miners are making come out at the cost of the tribals and the state exchequer, Shah Commission says, that who get the mining leases do not operate it themselves but give it to power of attorney holders or contractors. For the miners expenditure is not more than 45 per cent of the net value of production. The commission has recommended that in future half the net profits should be disgorged or equity share taken from the lessee for development of tribals. Even while the miners have turned billionaires, the commission notes how the labour- the displaced tribals - are ill-treated. “Mine owners do not pay more than minimum wages to the laborers even though their income is more than billions of rupees. They have no idea or intention of paying fair wages. Laborers are exploited and the object of seeing that locals benefit is frustrated.” The panel also records how the current system of allotting mining rights is based on political discretion of both the state and the centre, is open to corruption. I want to conclude my Quoting - Two roads diverged in the wood, someone took the road less travelled and it has made all the difference. Beliefs change into thoughts, thoughts change into words, word change into action, action change into behavior, behavior change into character and character changes into destiny, So arise awake and stop not till the goal is achieved. Therefore beware of your mind and beliefs. Best way to find yourself is loose yourself in the service of others. We are the repository of the millions and millions of People.

Thank You very much for giving me this opportunity. Clap. Did I not say it will be a treat to listen to Mr. Justice Gowda. His last couplet has summed everything and he has always been the man who has chosen the path less travelled. He has been the Guiding Light. One thing I came to know today is why did I loose a matter before

him in one of my case in Orissa whereby one after the other people succumbed before him. Unlike 2G in mining we know the source and it is quantifiable. In mining/gas extraction/forest it is notional nobody knows how much is mined and how much is mined. That's why it is also fuzzy and fuzzed figures leads to sec /black marketing and there the crime starts generation. M.B. Shah when started in mining scam, he started with Goa and gave detailed report and it was placed before forest court and all mining was directed to be closed and other operators learned from this and were scared and I came to appear for State of Orissa. Many operators came and surrendered and because they knew their fate and I realized the extent of the mining scam. Survey numbers were changed. Therefore it was very illuminating and enriching to hear and be here for this conference. Before concluding I want to say some-thing, it is a sahri in urdu, I have got English translation- If you have courage there is no wall. Very well said. Thank you Sir. Thank you. Can we have a big round of applause for Honb'le Gowda and Lalit Sir. Clap. Thank you all. Thank you Sir.