



**TWO DAY CONFERENCE ON
'INVESTIGATION OF FINANCIAL FRAUDS'**

Jointly organized by

Centre for Economic Crimes & Counter- Corruption Studies (CECCCS)

Sardar Patel University of Police, Security and Criminal Justice, Jodhpur

&

Rajasthan Police

Venue: Rajasthan Police Headquarters, Jaipur

September 8-9; 2016

INAUGURAL SESSION

Overview and objectives of the Conference: Shri S. Sengathir, IPS, Inspector General, CID (CB), Rajasthan Police welcomed the Chief guest for the inaugural session, the Vice-Chancellor of the University of Police, Security & Criminal Justice, Jodhpur, dignitaries on dais and participants.

The objectives of the workshop were as mentioned below:

- To make police personnel and public aware about different types of Financial Frauds.
- To discuss different specific laws/Acts which are specially enacted to deal with different types of Financial Frauds.
- To take an initiative towards making the police officials aware about the changing pattern of Financial Frauds.
- To understand the roles of different police officials while dealing with the Financial Frauds.
- To discuss the changing modus operandi in the realm of Financial Frauds.

“The central idea behind the Two Day Seminar is to provide a common platform to the experts in the field of financial frauds investigations having rich experience in the domain of financial crimes and police officials working in different positions across the state of Rajasthan; in order to familiarize the participants with the latest developments in the domain of the financial frauds. At the same time to provide them with the possible and appropriate course of action while dealing with the cases of financial frauds”

“The experts were requested all across the India to participate in the Conference and provide a deeper insight about the various types of Financial Frauds and to share their vital first hand experiences with the participants, who were majorly serving police officials from Rajasthan Police”

He also mentioned:

- “The most vulnerable section of the society are the poor people and lower middle class people while talking of the Financial Frauds.”
- “The main reason of the vulnerability because of Financial Frauds is Greed ie Illusion of making Quick Money.”
- “The civil society and the media shall do justice with their part of responsibility by making the people aware especially the most vulnerable and most exploited section of the society through timely intervention in form of mass awareness programmes with the help of appropriate media mix strategy ”

Address by the Vice- Chancellor of the University of Police, Security & Criminal Justice, Jodhpur: Dr. Bhupendra Singh, IPS, Addl. DGP, Government of Rajasthan

Dr. Bhupendra Singh welcomed the dignitaries on the dais, the organizers and the participants.

- He informed briefly about the different Centres that are functioning under the aegis of the University.
- The brief about the conferences and workshop conducted by the Centre for Economic Crimes and Counter Corruption Studies.
- “The seamless communication between the various stake holders is the key to prevent the possible financial crimes”
- “As mostly the people from economically poor background are the victims of such financial frauds, the Police officials should deal with such crimes swiftly.”
- “Police officials should develop appropriate SoPs while dealing with different types of financial crimes.”
- “These SoPs will give clarity of thought and direction to the concerned police official.”
- “The role of the media is vital to spread awareness and to prevent the financial frauds”

Introduction of the Centre for Economic Crimes & Counter-Corruption Studies (CECCCS): Shri Pankaj Kumar Singh, IPS, Addl. DGP, Government of Rajasthan and Executive Director, Centre for Economic Crimes and Counter Corruption Studies; welcomed the dignitaries on the dais, the organizers and the participants for taking time out of their busy schedule.

He also said that:

- “There has been and will always be a never ending race between the Police officials and the Criminals as the realm of financial crimes is not an exception.”
- “In order to build the confidence in the public the Police officials shall catch hold of the Criminals and ensure the timely and adequate punishment.”
- “Police should evolve and improve upon the SoPs especially while dealing with Economic crimes in the realm of Cyber space.”
- “The Police officials at the cutting edge of dealing with financial frauds should be trained properly with adequate provision to upgrade their learning and knowledge through timely inputs and interventions.”
- “The society has a major and positive role to play in this regard. The Police Officials need to be ahead of the curve in order to prevent possible instances of financial fraud”

Address by the Chief Guest: Shri Manoj Bhatt, IPS, DG of Police, Govt. of Rajasthan

Shri Manoj Bhatt said:

- “Police officials have their work cut out while dealing with the financial frauds. The need to resort to two way strategy in order to combat the menace of financial frauds. Firstly, along with media and civil society, the police officials shall strive for making people aware about the various types of financial frauds. Secondly the police official must have knowledge about various law/ acts pertaining to financial frauds”.
- “With the ever increasing financial well-being, the instances of financial frauds are expected to increase. Under such scenario the Police official need to be well trained to face the possible eventualities.”
- “In this regard, the conferences like this would go in a long way to build capacities at the appropriate levels in the Police forces”

Vote of Thanks: Shri S. Sengathir, IPS, Inspector General, CID (CB), Rajasthan Police thanked the Chief guest for the inaugural session, the Vice-Chancellor of the University of Police, Security & Criminal Justice, Jodhpur, dignitaries on dais and participants for their presence.

DAY - 1

TECHNICAL SESSION- I

CYBER FRAUDS

Presentation by: Mr. Kapil Garg (ADGP, State Crimes Record Bureau)

Mentioned below are the highlights of the Session:-

- Cyber frauds are the stark reality of the Virtual world.
- It involves any criminal action which either targets a computer or uses it to perpetrate a crime.
- Fraud - The crime of using dishonest methods or pretending what you are not.
- Types of Fraud- Traditional versus Cyber Space
 - Data is always involved in cyber crime
 - Virtual victim – data and the concerned person

- Limited by imagination of fraudsters
- Fastest crime and safest as anonymous and economical in nature

- Quantum of the Cyber Frauds:-
 - 74% increase in arrests
 - 54% criminals age 18-30
 - Out of 12248 cases, 65% pending investigation
 - Over 50,000 spam email reported to CERT-In every year
 - About 30,000 Indian websites hacked every year
 - Culprits –
 - 7% neighbors or family
 - 5% students
 - 3% employee
 - 2.5% business competitor

- Reasons for the cyber space to emerge as the preferred choice to perpetrate the financial crimes:-
 - Remote operations
 - Anonymity
 - Growing technology
 - Negligent users
 - Improved connectivity
 - Huge returns and low risk

- Hacking – access to private data.

- Phishing – contact through social media and obtain some sensitive details.

- Pharming – redirect you to a site where you should share your information.

- Emerging challenges in the Cyber space :-
 - Dark web
 - Dark net
 - TOR (the union router)
 - Crypto currency

Information Technology Act 2000 (Amended 2008) Salient Provisions:-

| Sl. No | Nature of complaint | Applicable section(s) and punishments under ITAA 2008 | Applicable section(s) under other laws and punishment |
|--------|--|--|---|
| 1 | Mobile phone lost/stolen | | Section 379 IPC upto 3 years imprisonment or fine or both |
| 2 | Receiving stolen computer/ mobile phone/ data (data or computer or mobile phone owned by you is found in the hands of someone else.) | Section 66 B of ITAA 2008 - upto 3 years imprisonment or Rupees one lakh fine or both | Section 411 IPC - upto 3 years imprisonment or fine or both |
| 3 | Data owned by you or your company in any form is stolen | Section 66 of ITAA 2008 - upto 3 years imprisonment or fine up to rupees five lakh or both | Section 379 IPC - upto 3 years imprisonment or fine or both |
| 4 | A password is stolen and used by someone else for fraudulent purpose. | Section 66C of ITAA 2008- upto 3 years imprisonment and fine up to Rupees one lakh Section 66D ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh | Section 419 IPC - upto 3 years imprisonment or fine Section 420 IPC - upto 7 years imprisonment and fine |
| 5 | An e-mail is read by someone else by fraudulently making use of password | Section 66 of ITAA 2008 - upto 3 years imprisonment or fine upto Rupees five lakh or both Section 66C of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh | |
| 6 | A biometric thumb impression is misused | Section 66C of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh | |
| 7 | An electronic signature or digital signature is misused | Section 66C of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh | |
| 8 | A Phishing e-mail is sent out in your name, asking for login credentials | Section 66D of ITAA 2008 - upto 3 years imprisonment and fine up to Rupees one lakh | Section 419 IPC - upto 3 years imprisonment or fine or both |

| Sl. No | Nature of complaint | Applicable section(s) and punishments under ITAA 2008 | Applicable section(s) under other laws and punishment |
|--------|---|--|--|
| 9 | Capturing, publishing, or transmitting the image of the private area without any person's consent or knowledge | Section 66E of ITAA 2008- upto 3 years imprisonment or fine not exceeding Rupees two lakh or both | Section 292 IPC - upto 2 years imprisonment and fine Rupees 2000 and upto 5 years and rupees 5000 for second and subsequent conviction |
| 10 | Tampering with computer source Documents | Section 65 of ITAA 2008- upto 3 years imprisonment or fine upto Rupees two lakh or both Section 66 of ITAA 2008 - upto 3 years imprisonment or fine upto Rupees five lakh or both | |
| 11 | Data Modification | Section 66 of ITAA 2008 - upto 3 years imprisonment or fine up to Rupees five lakh or both | |
| 12 | Sending offensive messages through communication service, etc. | Section 66A of ITAA 2008 - upto 3 years imprisonment and fine | Section 500 IPC — upto 2 years or fine or both Section 504 IPC — upto 2 years or fine or both Section 506 IPC — upto 2 years or fine or both — if threat be to cause death or grievous hurt, etc. — upto 7 years or fine or both Section 507 IPC — upto 2 years along with punishment under section 506 IPC Section 508 IPC — upto 1 year or fine or both Section 509 IPC — upto 1 years or fine or both of IPC as applicable |
| 13 | Publishing or transmitting obscene material in electronic form | Section 67 of ITAA 2008 first conviction - upto 3 years and 5 lakh Second or subsequent conviction - upto 5 years and up to 10 lakh | Section 292 IPC - upto 2 years imprisonment and fine Rupees 2000 and upto 5 years and rupees 5000 for second and subsequent conviction |
| 14 | Publishing or transmitting of material containing sexually explicit act, etc., in electronic form | Section 67A of ITAA 2008 first conviction - upto 5 years and up to 10 lakh Second or subsequent conviction - upto 7 years and up to 10 lakh | Section 292 IPC - upto 2 years imprisonment and fine Rupees 2000 and upto 5 years and rupees 5000 for second and subsequent conviction |
| 15 | Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form | Section 67B of ITAA 2008 first conviction - upto 5 years and up to 10 lakh Second or subsequent conviction - upto 7 years and up to 10 lakh | Section 292 IP - upto 2 years imprisonment and fine Rupees 2000 and upto 5 years and rupees 5000 for second and subsequent conviction |

- Future possibilities of financial frauds in Cyber space :-
 - More browser and web based infection
 - More sophisticated social engineering
 - More ransomware
 - BYOD vulnerabilities
 - New attack nectars

- Various useful resources to safeguard and to report against Cyber frauds:-
 - Rajcop App
 - Rajcop App
 - IT Act 2000-Cyber Law Mobile App
 - Cyber Crime Police Station, SCRB

TECHNICAL SESSION- II

ACCOUNTING FRAUD

Presentation by: Mr. A.Y.V. Krishna (Joint Director, CBI, Hyderabad)

Mentioned below are the highlights of the Session:-

- Major Corporate Frauds – World com , ENRON , Satyam
 - The exception was that except for Satyam all other companies liquidated post surfacing of the Scam.
 - Only Satyam survived.

- The Satyam case, 2008- All the relevant facets and dimensions.
 - Satyam was among top 4 Information Technology Services company.
 - Scam was majorly of falsification of revenues and margins to reflect the rosy picture about the state of affairs
 - Window Dressing
 - Common in scams among corporate frauds
 - Forging of the Books of Accounts.
 - Misrepresentation- Higher Revenue and Lower Expenses.
 - To reflect higher profitability

- Resulting into higher confidence of the shareholders and ever increasing value of the shares
 - Breach of Trust- Misguiding the shareholders.
 - Corporate Fraud- As Satyam, a corporate entity does wrong with proved intentional dishonesty.
- Reasons for the Satyam Scam, 2008:-
- Greed
 - To match market expectations
 - Intense feeling of competition
 - Individual glory
 - Failure of regulators
 - Inadequacies in the Companies Act, 1956
- Modus Operandi of the Satyam Scam :-
- Fake invoice
 - Secret Codes
 - Unauthorized Approvals
- Peculiarities and Technicalities of the Satyam Scam-
- No hard copies
 - Computer based and computer driven
 - Back-ups of hard disk
 - Network logs
 - Application logs
- The statement by B. Raju- It was like riding a tiger, not knowing how to get off without being eaten."

TECHNICAL SESSION- III

CREDIT CARD FRAUDS

Presentation by: Mr. Rajesh Nirvan (IGP, PM&W)

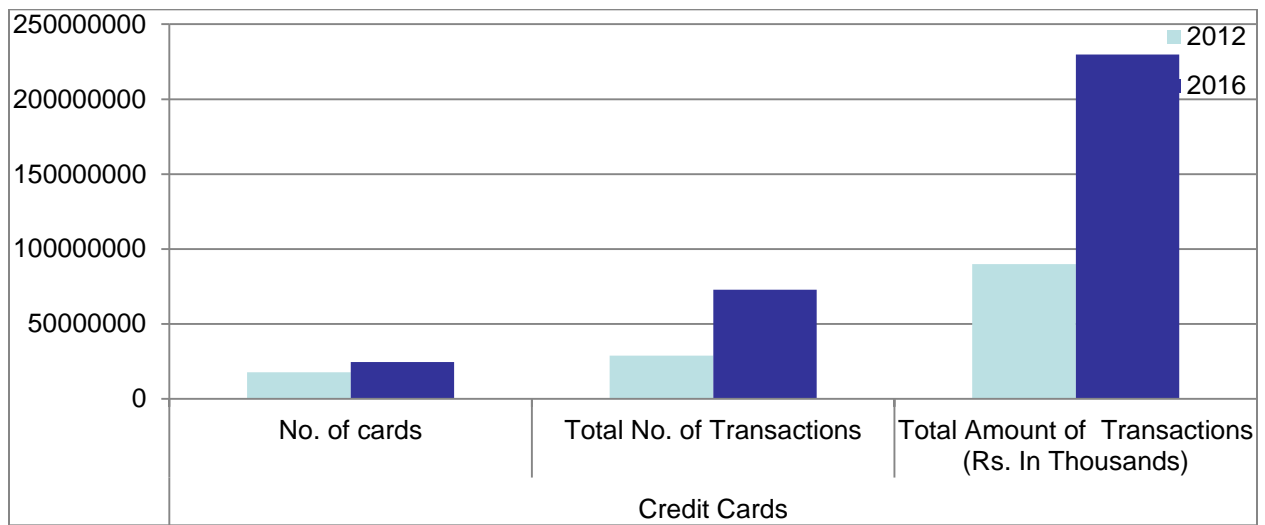
Mentioned below are the highlights of the Session:-

- Card Frauds are done through various means like:

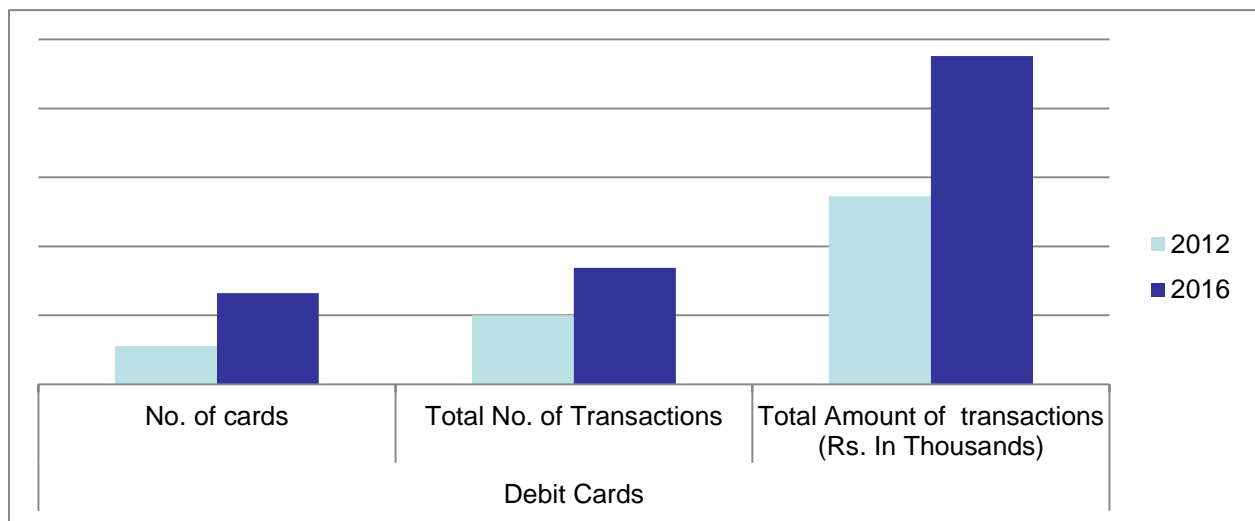
- Dumpster Diving
- Vishing
- Phishing
- Skimming
- ID Theft
- Shoulder Surfing
- Shimming

Increasing importance of Plastic Money:-

Credit Cards



Debit Cards:-



- Few precautions to safeguard against the frauds:-
 - Never disclose any information about the credit card.
 - Never answer any call, even if the caller claims to be calling from the bank.
 - Receive your new card and sign on the back of it.
 - Record all account numbers and company contact information and keep the information at a safe place.
 - Never write down the PIN anywhere.
 - Never give the PIN to anyone.
 - Call your card company immediately and give information about lost or stolen cards or PIN numbers.

- In case of the credit card fraud, always report the case to the police.
 - Get a police report.

EVERY POLICE STATION GETS 3-4 COMPLAINTS A DAY

Every police station, on an average, gets three to four complaints on cybercrime. Police stations in the city lack infrastructure and expertise to investigate cybercrime cases.

CREDIT, DEBIT CARD FRAUDS ON THE RISE

| Year | Number of Cases |
|------|-----------------|
| 2015 | 255 |
| 2014 | 158 |
| 2013 | 32 |
| 2012 | 8 |

STATE'S CYBERCRIME CONTROL PROJECT

- The project was first drafted for Mumbai but was later extended to the state, with every district police having the infrastructure to deal with the menace
- Formation of four cyber cells equipped with latest hardware, software and tools
- Developing a force of 1,000 trained cyber cops
- Special fast-track courts dedicated to cyber crime cases
- Training prosecutors and judicial officers
- A Computer Emergency Response Team (CERT)

POLICE CHIEF MEETS REPRESENTATIVE OF 19 BANKS

Commissioner of police Ahmed Javed met senior officials of as many as 19 banks, including MDs, CEOs, directors and senior risk managers to discuss measures taken for data security. The meeting was held at the police commissioner office. Possible measures on data security that banks can put in place internally and co-operation with police in investigating cyber crimes were discussed

CITY POLICE YET TO GET FOUR CYBER CELLS, BUT GETS A DCP CYBER

Though the cyber crime cases are increasing manifold, city police are awaiting approvals for four CCICs which will look after cybercrimes of south, east-central and north regions. However, on Monday, city police got its first deputy commissioner of police (DCP)-cyber, M Rajkumar

BKC CYBER CRIME POLICE STATION OVERBURDENED

City's only cyber police station has only 15 officers, including a senior inspector and two senior inspectors

Since only an officer of inspector rank can be official investigating officer of a crime

under the IT Act, the two PIs are overburdened with over 100 cases each

Around 250 FIRs have been filed at the BKC cybercrime police station this year

In order to tackle the manpower issue, the police sent a recommendation earlier this year asking for amendment to section 78 of the IT Act and allow officers of police sub-inspector (PSI) rank and above to probe cases

IN CASE OF CREDIT CARD FRAUD

THE JUSTICE HOOPS

- **BANK**
What it costs? **Nil**
Time it takes: **30-45 days**
- **BANKING OMBUDSMAN**
What it costs? **Nil**
Time it takes: **30 days**
- **APPELLATE AUTHORITY**
What it costs? **Nil**
Time it takes: **Reserve Bank of India says it replies as soon as complaint is received**
- **COURT**
What it costs? **Depends on the lawyer's fee**
Time it takes: **Can extend into many years**

TIPS TO AVOID FRAUDS

- Use the virtual keyboard to key in the password
- Change your password frequently
- Use a combination of numbers, alphabets and special characters to make your password strong
- Go for credit cards that are chip-based as they are more secure as compared to those having magnetic strips
- Before logging in, check if the site has https and the lock sign in the address bar. In https, "s" stands for secured



➤ Legal provisions dealing with the credit card frauds :-

- IPC – Section 419, 420
- IT Act – Section 66C, 66D

TECHNICAL SESSION- IV

BANKING FRAUDS

Presentation by: Mr. Hemant Priyadarshi (IGP, Jaipur Range)

Mentioned below are the highlights of the Session:-

- RBI has defined the term “fraud” in its guidelines on frauds which reads as under.
“A deliberate **act** of omission or commission by any person, **carried out in the course of a banking transaction or in the books of accounts** maintained manually or under computer system **in banks**, resulting into **wrongful gain** to any person for a temporary period or otherwise, **with or without any monetary loss to the bank**”.
- Types of Frauds:-
 - Account opening fraud
 - Cheque kiting
 - Cheque fraud
 - Counterfeit securities
 - Embezzlement
 - Computer fraud
 - Loan fraud
 - Money laundering fraud
 - lottery fraud
 - Letters of Credit
 - Advanced Fees Fraud
- Frauds related to the advances portfolio accounts for the largest Share of the total amount involved in frauds in the banking sector. (Involving amount of Rs. 50 crore and above)
- RBI has clearly indicated that fraud risk management, fraud monitoring and fraud investigation function must be owned by the bank’s CEO, audit committee of the board.
- In respect large value frauds, the special committee of the board are CMDs, CEOs, audit committee and the special committee evolving robust fraud risk management systems.

- Year-wise and amount of fraud cases in the banking sector

| Sl. No. | Year | No. of cases | Total amount (in Rs Crores) |
|---------|----------|--------------|--------------------------------|
| 1 | 2009-10 | 24791 | 2037.81 |
| 2 | 2010- 11 | 19827 | 3832.08 |
| 3 | 2011- 12 | 14735 | 4491.54 |
| 4 | 2012- 13 | 13293 | 8646.0 |

- **Target:** Minimize Losses, Least Adverse Publicity, Preserving of material Evidence, Effective Legal Action
- **Agencies:**
 - District Police
 - CID (CB),
 - Economic Offences Wing (EoW)
 - Special Fraud Investigation Office (SFIO)
 - CBI (fraud amount more than 3 crores in Public Sector Banks)
- **Important Steps in investigation:-**
 - Preliminary Enquiry (if required, permitted in SC judgment of *Lalita Kumari*) to ascertain cognizable offence, N.I Act, Civil matter?
 - FIR: Proper drafting is key (Bhajan Lal case *1992 AIR 604, 1990 SCR Supl. (3) 259*) moneyed suspects.
 - Understand the banking methodology, co-opt experts(Satyam case)
 - Searches, collection of documents including hard disks (proper custody , 65B I. EV. Act, 2A Bankers Books of Evidence Act), imaging of hard disk.
 - Necessary follow up action with other agency
- **Key to investigation**
 - Immediate collection of documents, evidence about dishonest intention knowledge, *mensrea*.

- Following are the 3 cases which were discussed:-
 - Letter of Credit (LC) Fraud
 - Warehouse Receipt Fraud
 - Union Bank Case

DAY - 2

TECHNICAL SESSION- V

GENERAL INSURANCE FRAUDS

Presentation by: Mr. Rakesh Kumar (GM & CVO Oriental Insurance)

Mentioned below are the highlights of the Session:-

- **Insurance** is the equitable transfer of the risk of a loss, from one entity to another in exchange for payment. It is a form of risk management primarily used to hedge against the risk of uncertain loss.
- The insured receives a contract, called the insurance policy

- Subject Matter of Insurance- Broadly 4 Groups:-
 - Insurance of Property (Motor, Building, Plant, Machinery etc.)
 - Insurance of Person / Life (Personal Accident, Medi-claim etc.)
 - Insurance of Liability (Motor Third Party, Workman Compensation etc.)
 - Insurance of Profit (Loss and Profit, Advance Loss of Profit)

- One of the Important Principle of General Insurance- Indemnity
 - Section 124 under Chapter VIII of Indian Contract Act 1872 "Contract of indemnity" defines it- "The transaction involves the Insured assuming a guaranteed and known relatively small loss in the form of payment to the insurer

in exchange for the insurer's promise to compensate (indemnify) the insured in the case of a financial (personal) loss.

➤ Ingredients of Contract-

- Offer / Proposal
- Acceptance
- Consideration
- Final Contract

➤ In Insurance Contract, there is a special Ingredient between Offer and Acceptance, which is defined as Underwriting.

➤ The acceptance of proposal / offer is based on the analysis of risk involved in that particular proposal.

➤ Premium is also decided on the basis of risk involved in that proposal

➤ Insurance Policy

Audit Details Query

The Oriental Insurance Company Ltd.

Policy Status : New Policy / Status : Complete

| | | | | | | |
|----------------|------------------|----------------------------|-------------------|-----------------------|---------------------|---------------------|
| Policy Type | MOT-PLT-002 | LIABILITY ONLY POLICY | Policy Number | 151300/31/2014/854 | Item No. | 0 |
| Business Type | 1 | Direct without coinsurance | Proposal Number | R/151300/31/2013/7312 | | |
| Customer | AA00000000 | GENERAL CUSTOMER | Insured | 19872786 | M/S TRIVEDI BUS SEF | Insured Details |
| Source Type | 1 | Direct | Dev. Officer Code | NA000000267 | LGF SERVICES LTD | Premium Comp. Sheet |
| Source Code | | | | | | |
| Cover Note No. | | | Cover Note Date | | | |
| Period From | 22/04/2013 00:00 | | To | 21/04/2014 23:59 | | |
| Mode Of Pay | OT | Others | Premium Calc Type | 3 | Normal/Annual | |

KYC Verified Banned Entities

State Road Transport (Y/N)

Do Not Renew

Modify End.Date

➤ **The position of power can be misused** at any stage during the process of applying, buying, using, selling, underwriting insurance or while staking a claim which can be broadly categorized as under :-

1. Pre Insurance otherwise known as application
2. Post Insurance - claims

➤ **Procedure of General Insurance Claim-**

1. Intimation by Insured for accidental loss to subject matter of Insurance
2. Registration of Claim by Insurer
3. Deputation of Surveyor / Investigator for assessment of liability of Insurer
4. Assessment and submission of Survey report by Surveyor
5. Scrutiny of Claim file
6. Letter to Insured regarding assessment of loss and to submit required information / papers.
7. Approval of Claim by the Competent Authority, after receiving the complete information / papers
8. Settlement of Claim

➤ Mentioned below is the case study that was discussed:-

Tempering with the Computer and Generation of Bogus Policies under which claims were paid- 1998

TECHNICAL SESSION – VII

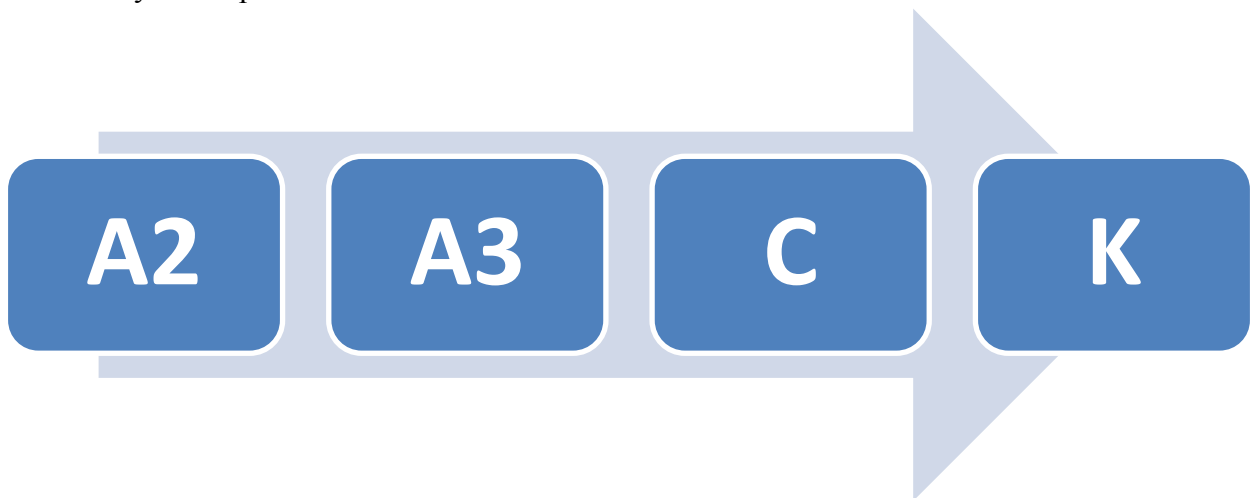
SHELL COMPANIES

Presentation by: Mr. Vivek Priyadarshi (SP,CBI)

Mentioned below are the highlights of the Session:-

- **Shell Company:** A company with no significant assets or ongoing / regular business activity formed as a vehicle to raise funds before starting operations, or to attempt a takeover, or to act as a front for an illegal business, etc.
- Nicknames of shell companies are :-
 - ‘Phantom Companies’
 - ‘Anonymous Companies’
 - ‘Ghost Companies’
- A shell company is not necessarily for illegal purpose.
- A Global Financial Integrity report found that shell companies are used to send over a \$1 trillion annually out of emerging economies.
- Over 200,000 shell companies involved in Panama Papers leak
- In May 2016, authorities uncovered a fraud, wherein some individuals cheated the government and banks of several crores of rupees using a maze of 24 ghost companies operating from a single branch of a bank in Delhi.
- SIT observed that investments from Cayman Islands, a tax haven, alone amount to Rs. 85,000 crore in India, highlighting the role of tax havens in money laundering.
- Shell Companies : Characteristics
 - Shell companies are hollow & do nothing but manage the money inside them
 - Lawyers or accountants or dummies are listed as directors
 - Difficult to figure out the ultimate beneficiaries
 - ‘Nominee’ services – people hired to allow their names on the registration forms, esp. in Tax Havens

- The forms for incorporation are often the only public proof of a shell company's existence - No phone number, physical address, company logo, contact person, etc.
 - Beneficial owner - the real people who ultimately own or control a company behind multiple layers
 - Special categories: LLCs, Cells of a company, etc.
- Various purposes for establishing Shell Companies:
- Pre-operation financing / special purpose vehicle to raise funds, etc.
 - To conduct a hostile takeover
 - To act as a front / to disguise business ownership from the public or the business rivals or law enforcement
 - Tax Evasion / avoidance, including round-tripping through tax havens
 - To Launder money – Black Money to White & vice versa
 - Accommodation Entries (*Jamakharchi*) for fraudulent activities
- Detection of Frauds-
- Focus on significant transactions
 - Trend Analysis
 - Unusual debits/credits in accounts
 - False credits, with corresponding debits, from/ to dummy accounts, etc.
 - Ratio Analysis
 - Abnormal numbers / data
 - Historical Comparisons
 - Investigator's Intuition & Common Sense
- Case Study : 2G Spectrum Case



‘A2’ : a partnership firm of ‘A’ Group of companies, A1 got Telecom License

‘A3’ : A Shell Company of A Group of companies

‘C’ : A company in the main stream business of Films

‘K’ : Target company related to accused Telecom Minister’s Party

TECHNICAL SESSION – VIII

MULTI LEVEL MARKETING FRAUDS

Presentation by: Mr. Balwinder Singh (IPS Retd.; Former Special Director, CBI) and Director, Centre for Economic Crimes and Counter-Corruption Studies

Following were the highlights of the session:-

- Less educated and if educated then less aware investors fall prey to such frauds.
- Attractive interest rates, good services and high profile of companies create credibility and confidence in the minds of such investors.
- Fraudulent mobilisation includes public deposits in the guise of:-
 - Receiving advance,
 - Provision of some services,
 - Collective investment schemes and
 - Issue of preference shares as private placements and
 - Functioning as NBFCs(Non- banking Financial Companies)
- Enrolment of members can be through both-
 1. Pyramidal Enrolment
 2. Normal enrolment of commission agents
- Compensation plans – these are designed to inevitably motivate the participants in the scheme to concentrate on recruiting more participants to make quick and easy money.
 - Such schemes enrich the company and the top of the pyramid participants (TOPPs) at the cost of vast majority of the participants who are at the bottom two levels of the pyramid.
- Use of internet - Fraudulent companies based abroad are also exploiting gullible Indian public by offering certain ‘services’ through internet.
- Effective coordination between Central & State agencies would help state police in early detection of frauds and would help Central agencies in better regulation.

VALEDICTORY SESSION AND VOTE OF THANKS

The Chief Guest for the Valedictory Session- Shri Ajit Singh, DGP, Prisons, Government of Rajasthan. Shri Ajit Singh congratulated the University, Rajasthan Police and the Centre for coming up with the conference having high degree of relevancy to the Police officials.

Shri Ajit Singh dealt with:-

- Broadly two topics- the Bitcoin and Hawala Network
- “Hawala networks are in existence since time immemorial”
- “The main reason for existence of Hawala networks is lack of penetration of Banking facilities across geographies along with ease of doing such transaction”
- “Over the period of time these networks are used to transfer ill-gotten money, black money and dirty money”
- “The Bitcoin, also called as Crypto currency, has emerged as a medium of exchange over the cyber space”
- “Although Bitcoin lacks the backing of an official government and are very volatile in their nature”

Follow up of the Conference- Shri S. Sengathir, IPS, Inspector General, CID (CB), Rajasthan Police; thanked the Chief guest of the session, the Vice-Chancellor of the University of Police, Security & Criminal Justice, Jodhpur, dignitaries on dais and participants. Shri Sengathir, covered the central theme of all the sessions briefly.

Vote of Thanks: Dr. Bhupendra Singh, IPS, Addl. DGP, Government of Rajasthan & Vice-Chancellor, Sardar Patel University of Police, Security and Criminal Justice, Jodhpur thanked the Rajasthan Police, dignitaries on the dais, the organizers and the participants on behalf of the University and the Centre with hope of further collaboration and coordination between the Rajasthan Police and the University.

The conference got concluded with distribution of the certificates to all the participants.