

# Telecom Fraud Management & Revenue Assurance Conférence 2010

## Investigation & Mitigation Techniques

Presented by:

**Anurag Parashar, CFE**  
Fraud Investigations & Vigilance  
Bharti Airtel Ltd.

# Index:

---

- How to create value in Investigations & Fraud Management.
- Latest Modus Operandi of Fraudsters & evolution.
- Best Practices in uncovering the Modus Operandi.
- How to keep a tap on Policy Violations.
- Best ways for improving existing policies.
- Preparation, collection and preservation of evidence.
- Most commonly encountered frauds affecting Corporate organizations.

# Creating value by Investigations & FM

---

## Approach

- Proactive instead of Reactive.
- Emphasis on Preventive instead Punitive.
- Fact Finding instead of disciplinary action oriented.

## Orientation

- Pick n choose with a focus on revenue leakage instead of disciplinary proceedings.
- Strategic instead of operational.
- Always be directed towards process improvements in addition to fixing the responsibility for violations.

## Investigation/ FM

- Time bound with quality output.
- Clearly defining what went wrong & why in addition to who did it.
- Recommendations should be feasible and acceptable by business.
- Shall be in correlation to the Financial figures.

## Engaging with Business

- Inculcating a No Surprise Culture.
- Should be visible & accepted as Business Enabler.
- Assisting business in process reviews especially with inputs on possible frauds, upcoming trends and possible mitigation plans.
- Regular MIS on ongoing issues.

# Latest Modus Operandi

---

- Tech Savvy.
- Social Engineering.
- Backed up with data.
- Targeting areas where high yield is visible / expected.
- High risk taking.
- Selective in picking the target – focus on the process / control gaps.

## Best Practices in uncovering the Modus Operandi:

- RCA based on 5 WHY's.
- Think like a fraudster and proceed.
- Use of appropriate technology and Subject Matter Expert.
- Engage with operational level staff in business units.
- Regular updation of the knowledge and skill sets.

# Tap on Policy Violations:

## Awareness

- Wide coverage including employees/ channel partners/ vendors/ suppliers & customers on policies.
- Multiple approach for creating awareness – e learning modules, personal interactions, posters etc.

## Building a culture of Compliance

- Setting the tone from the top by Management.
- Promoting strict adherence to policies.
- Setting Zero Tolerance towards violation of critical policies.
- Recognition and reward for showing exemplary contribution. This would also motivate others in the system/ organization.

## Continuous Monitoring

- Regular / continuous monitoring of abnormal transactions leading to policy violations.
- Identification of most commonly encountered trends of violations.
- Analysis/ audit/ investigation of the outputs of the above activity.
- Fraud Risk Assessments of key processes and applications.

## Building/ Implementing Controls

- Systemic/ technical/ application based controls.
- Amendment of Policies if required.
- Increased Segregation of Duties.
- Realignment of thresholds.
- Applying consequence management.

# Policy Improvements:

---

## Why an improvement is required:

- To be in accordance with fast changing business requirements & market.
- To meet the industry bench marks globally.
- To acquire & cater a wide range of customers from different geographies and spending power.
- To withstand the high attrition rates without compromising on the Organizational values.

## Best ways for Policy Improvements:

- IT enabled approach – especially to take care of issues like SOD, DOA etc.
- Survey based – especially employee/ channel partner oriented wherein ideologically policy should be defined and implemented after having survey / discussion with stake holders.
- Cross functional approach.
- Risk based – in order to arrest the reoccurrence of violations experienced in past.

# Collection & Preservation of Evidences:

---

As an Investigator one should always remember –

## Do's

- Preservation of the evidence is the first step in any investigation.
- Look for evidence which shall be substantiated with data in any form.
- Written instead of verbal or here say.
- Preservation of evidences should not be person dependent.
- Specific in picking the evidence.
- Should prefer storing the evidence in electronic format wherever possible.
- Should bring in an expert whenever the case demands.
- Should be in sync with applicable laws and regulations.

## Don'ts

- Collect loads and loads of data in the name of evidence.
- Delay in collecting the evidence.
- Compromise on the safety / custody of the evidence.
- Don't let the delinquent understand what you as an investigator is going to produced as an evidence.

# Most commonly encountered Frauds:

---

In addition to Telecom Frauds we as Investigators/ auditors should also keep an eye on the areas like Human Resources, Supply Chain & Finance. These core functions are an integral part of any corporate body and are highly prone to fraud. Some of the indicators of suspected fraud which might be existing in any organization as follows:

Human Resources	Supply Chain	Finance
Ghost Employees	PO/ invoices processed in respect of one time vendors more than once.	Duplicate payments.
Employee Vendor linkage on common parameters	PO split with same vendor, quantity and item	Journal entries where creator is approver
Financial transactions in favor of terminated employees	Duplicate purchase orders – same item & quantity	Asset disposals at Nil or Negative value
Employees having same bank accounts	Intentional delay in invoice processing	Abnormal delays in payments/ payments made prior to the due date.
Employee Hire Volume	Good received Vs. invoice processing	Depreciation of assets

---



**Queries?**

---

Anurag Parashar  
Mobile No: 9810668115  
Email: [Anurag.Parashar@airtel.in](mailto:Anurag.Parashar@airtel.in)