

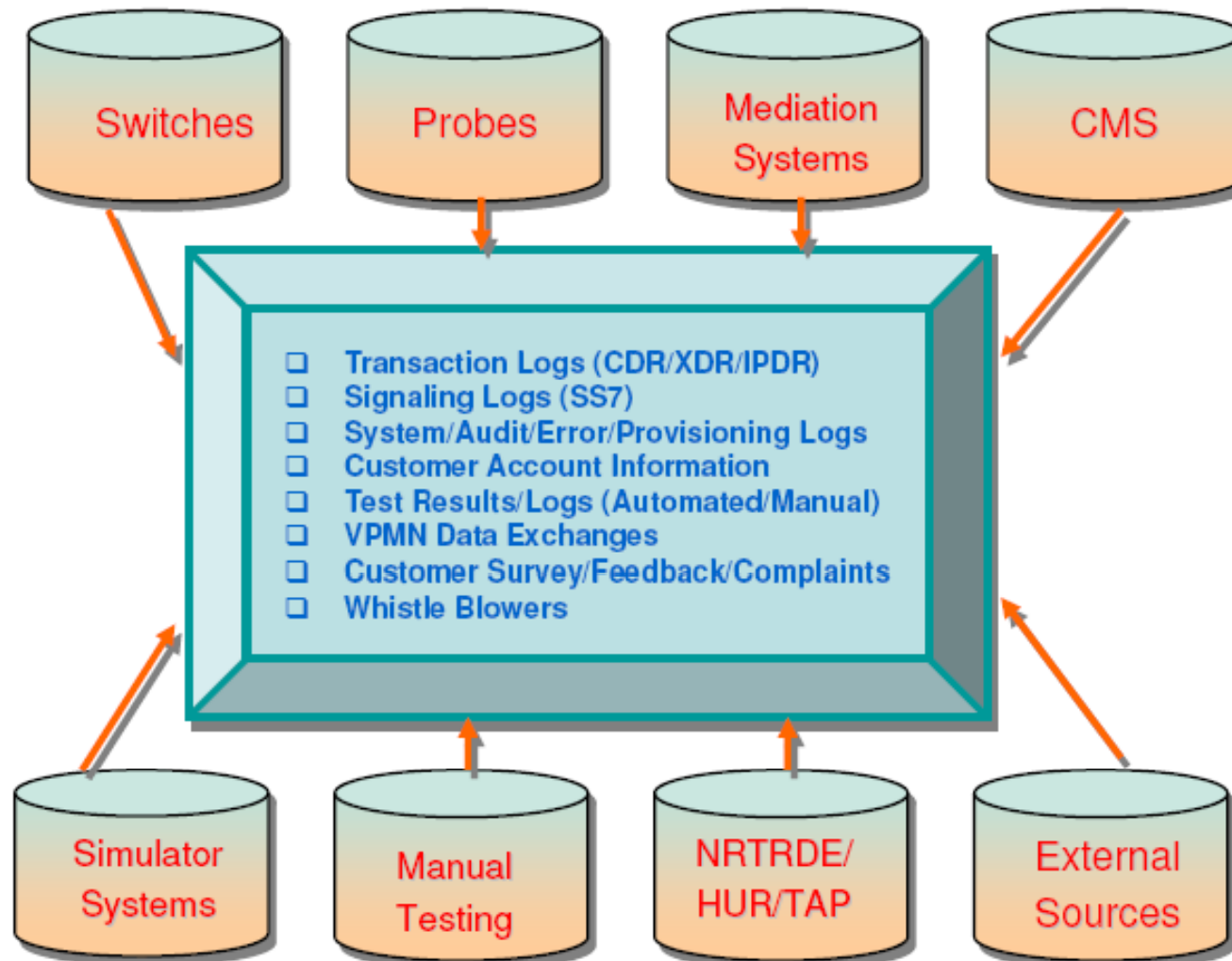
# Internal Fraud Mitigation Strategies

Confidential

The only time a Tata Indicom Phone won't be accessible.  
Please switch off your mobile phones during the presentation.



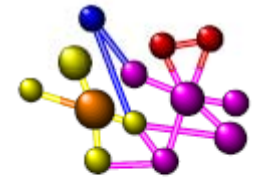
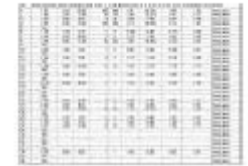
# FRAUD Reference Data Sources



# Identifying FRAUD



- Transaction Records Analysis (e.g. CDR)
- Discount Components
- Demo Plans
- Hyper-Linking Process of Analysis
- Referencing against submitted Documents
- Call-Out Verification
- On-site/Off-site Investigation
- Regular Account level Bill Checks.
- Fraud Forums/Partner Collaborations
- Customer Complaints Analysis and Investigation
- Whistle Blowers



# FRAUD Indicators

- Revenue Behavior
- Transaction Volume
- Location
- Billing
- Services acquired
- Configuration Errors
- Suppressed CDRs / Billing
- Erroneous Data Records
- Switch Overloading
- Equipment/System Outages



# FRAUD Detection Tools & Techniques



- Real-Time Monitoring Tools
- Manual Profiling by Team
- Testing and Simulation
- Filtering and Normalization Techniques
- Segmentation Techniques
- Scoring Techniques
- Bashing and Trending Techniques
- Case Correlations
- Post Validation Methods
- Use of Alerts/Alarms and self triggered
- Notifications/escalations



# Fraud Mitigation

No Business, No Risks.



# No Business, No Risks.

- Ironically, Every Business success is the cause of risk
- More success, more money, more fraud
- Easiest way to reduce fraud is to reduce business
- Don't laugh. This is what most FC and HR people do, unintentionally



# Fraud Categories

## Four Categories of Fraud :

- Operational Fraud
- Compliance Fraud
- Financial Fraud
- Strategic Fraud



# Levels of Impact (Fraud)

<u>Likelihood</u>	<u>Impact</u>	<u>Financial Impact</u>
<b>5. Very high</b>	<b>Very Serious</b>	>100K
<b>4. High</b>	<b>Serious</b>	51K-100K
<b>3. Medium</b>	<b>Moderate</b>	25K-50K
<b>2. Low</b>	<b>Minor</b>	6K-25K
<b>1. Very Low</b>	<b>Insignificant</b>	0-5K



# Fraud Root Causes

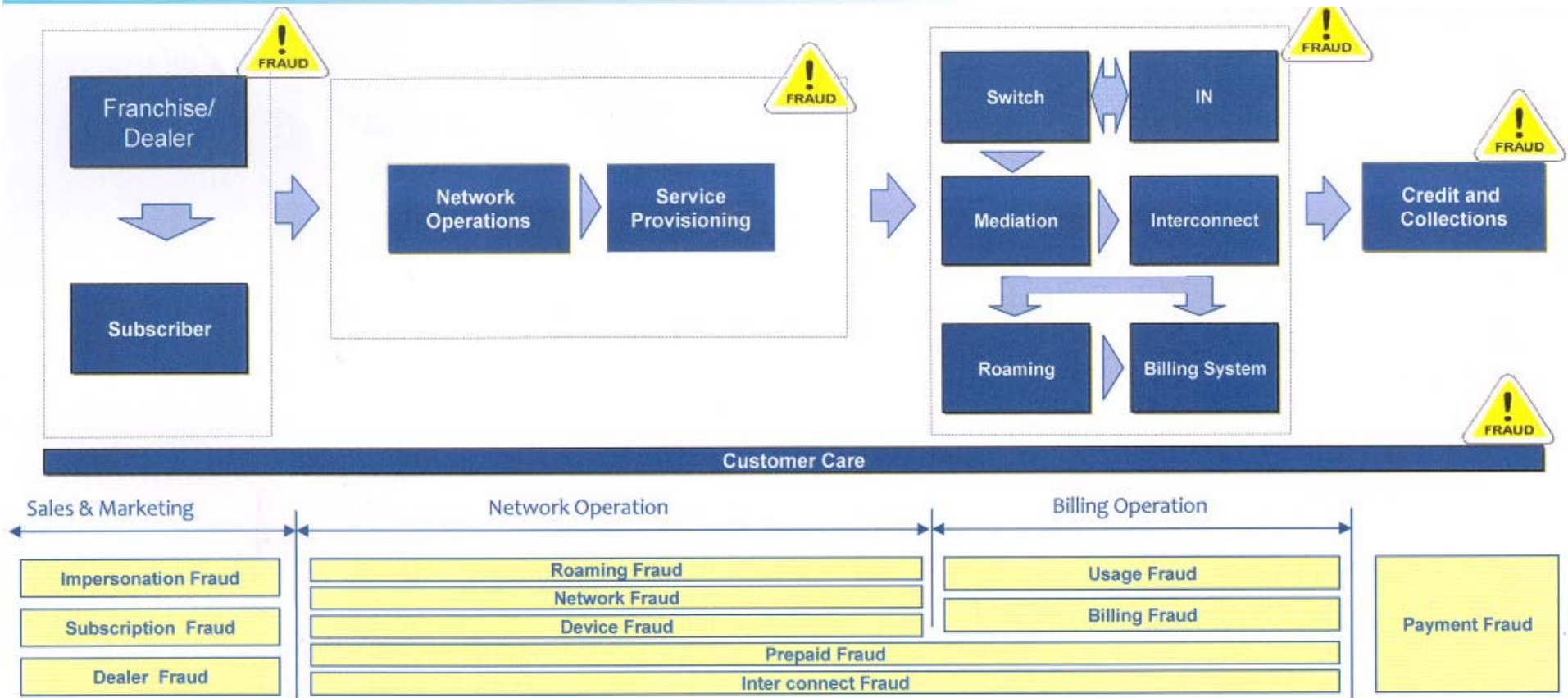
- Policy problem
- People problem
- Unavoidable problem



# Revenue Cycle Fraud



# Fraud in Revenue Cycle of Telecoms



Major classifications of frauds in revenue cycle are related to:



# Sales and Marketing Frauds



## Key Features

- Entry level frauds
- Comprises typically of Impersonation fraud and Subscription fraud
- Mostly committed by customers or through his/her accomplice in the Telecom operation

## Areas where frauds can occur

**Dealer Selection**

**KYC Documents**

**Customer Verification**

**Fictitious Sales**

**Premium Number Allocation**

**Sales Commission Processing**

### Client's issue



Abnormal high usage in the international long distance segment

### Our Approach

- Formed a team comprising of process, forensic and technology teams
- Data analysis and process review to identify subscribers with fraud patterns
- Identify/track suspects and insider involvement through investigations and reviews
- Identified and help mitigate the risks in processes and systems that caused this fraud

### Conclusion

- Retailers and internal employees were responsible for the frauds
- Connection provided with forged documents
- Activation without credit verification / bad credit rating
- Inadequate evaluation of franchisees and CV agencies



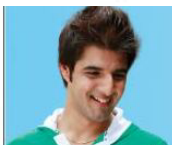
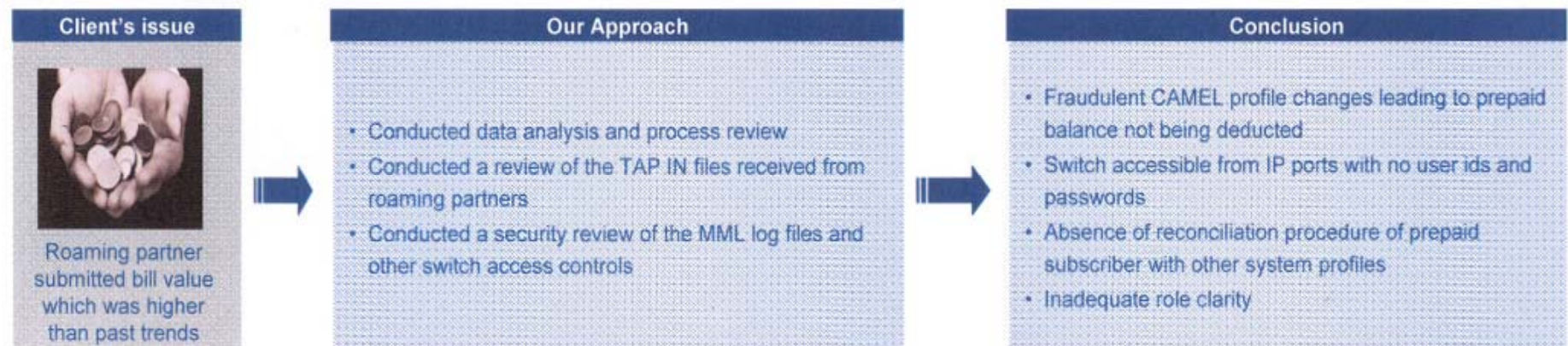
# Network Operation Frauds



## Key Features

- Prevalent primarily in high value services
- Undertaken by customer or third party ( sometimes with the help of internal members)
- Financial gain, eavesdropping on conversation, service outage, industrial espionage etc

## Areas where frauds can occur



# Billing Operation Frauds



## Key Features

- Exists due to weak processes and controls
- Systems impacted by frauds are post paid billing, IN, mediation, inter connect and roaming
- Carried out predominantly by employees

## Areas where frauds can occur

Validity  
Extension

Removal of  
Prepaid Flag

Suppression  
of Billing  
CDRs

Billing  
Configuration

Voucher  
Activation /  
Top-ups

Toll free /  
Special  
Number  
Configuration

Mediation  
Filtration

### Client's issue



High number of international calls in a short period and unauthorised pre-paid to post paid conversions

### Our Approach

- Conducted a review of the organisation structure
- Review of the relevant processes and systems
- Conducted interviews and used external field intelligence
- Used data analytics and system log analysis tools

### Conclusion

- Employee ids were used to assign post paid service package and tariff plans to prepaid numbers
- Delay in monitoring roaming HUR
- Gaps in revenue assurance processes
- External and internal persons responsible for this fraud were identified



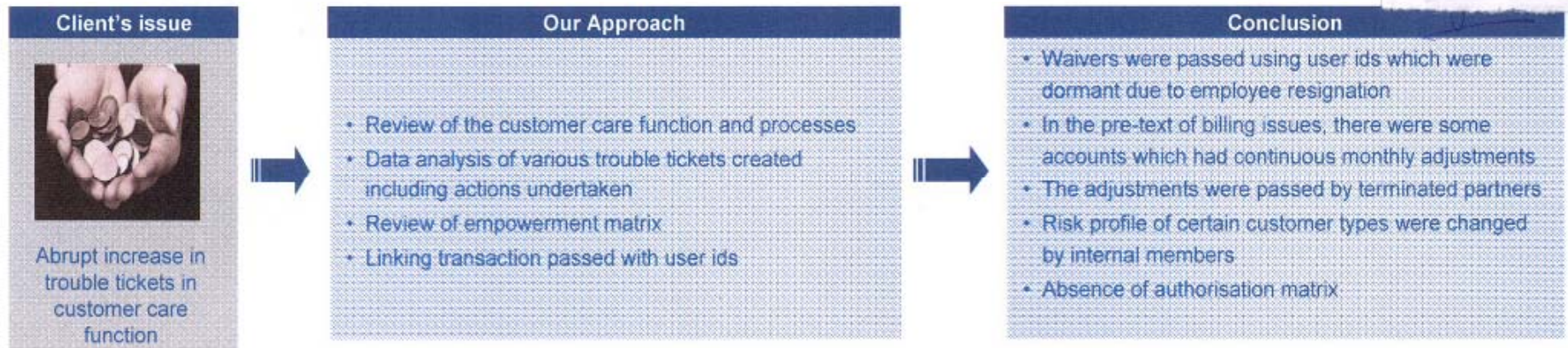
# Credit and Collection Frauds



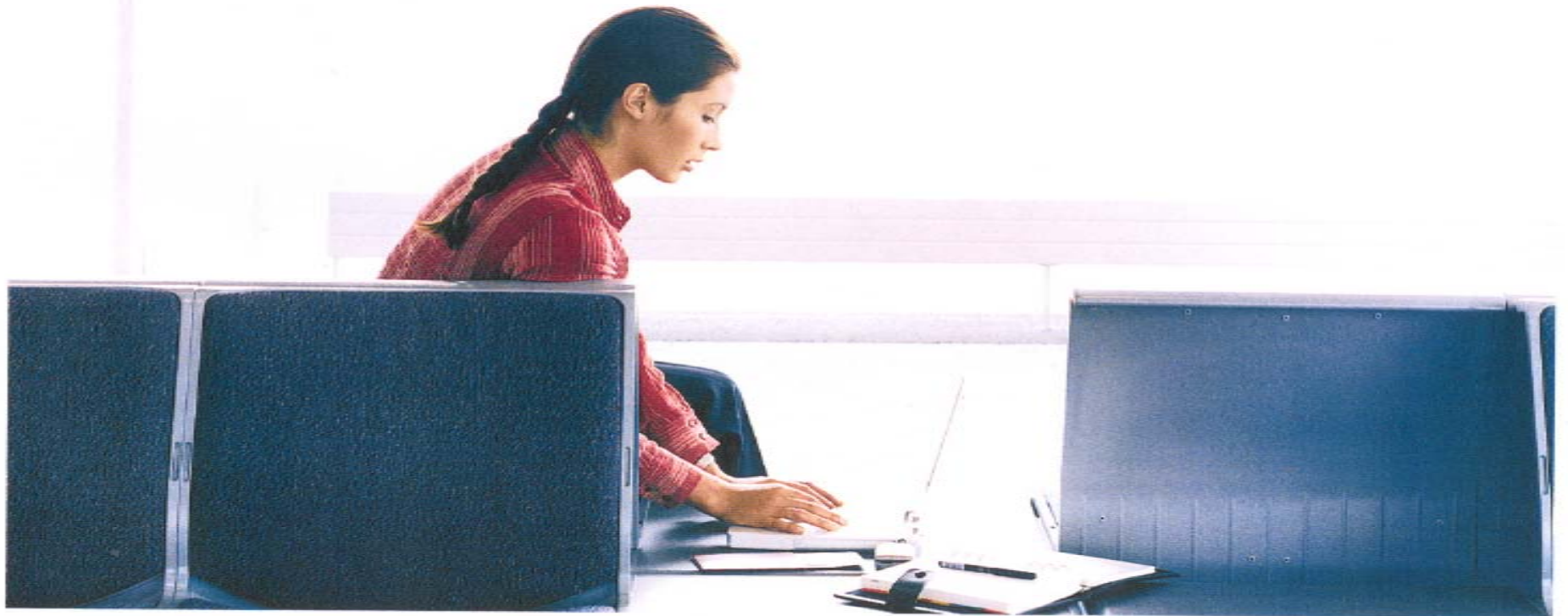
## Key Features

- Residual impact of all kind of frauds – non payment
- Fraudster take advantage of gaps in financial security procedures

## Areas where frauds can occur



## Procurement Fraud Scenarios



# Scenario 1



## Procurement of Diesel for DG Sets at tower sites

A bogus quotation submitted by a vendor clearly revealed by the mark and confirmed through site visits



[Redacted] **SERVICE STATION**

I.O.C. Dealer

New Mental Hospital Road [Hosur Road] Bangalore-560029.

Date: 10/01/2009

To,

M/s. [Redacted]

Bangalore, 560001.

Kind Attn: Mr. \_\_\_\_\_

Dear Sir,

Subj: Consumables quotation for 750 KVA DGset.

Running Diesel and Engine Oil every 250 hours running Oil Filter, fuel filters, radiator coolant oil, Transport charges from Petrol bunk to Raheja Tower [Your site] and filling charges Credit of on pro rata basis @ Rs. 4600/- per hour.

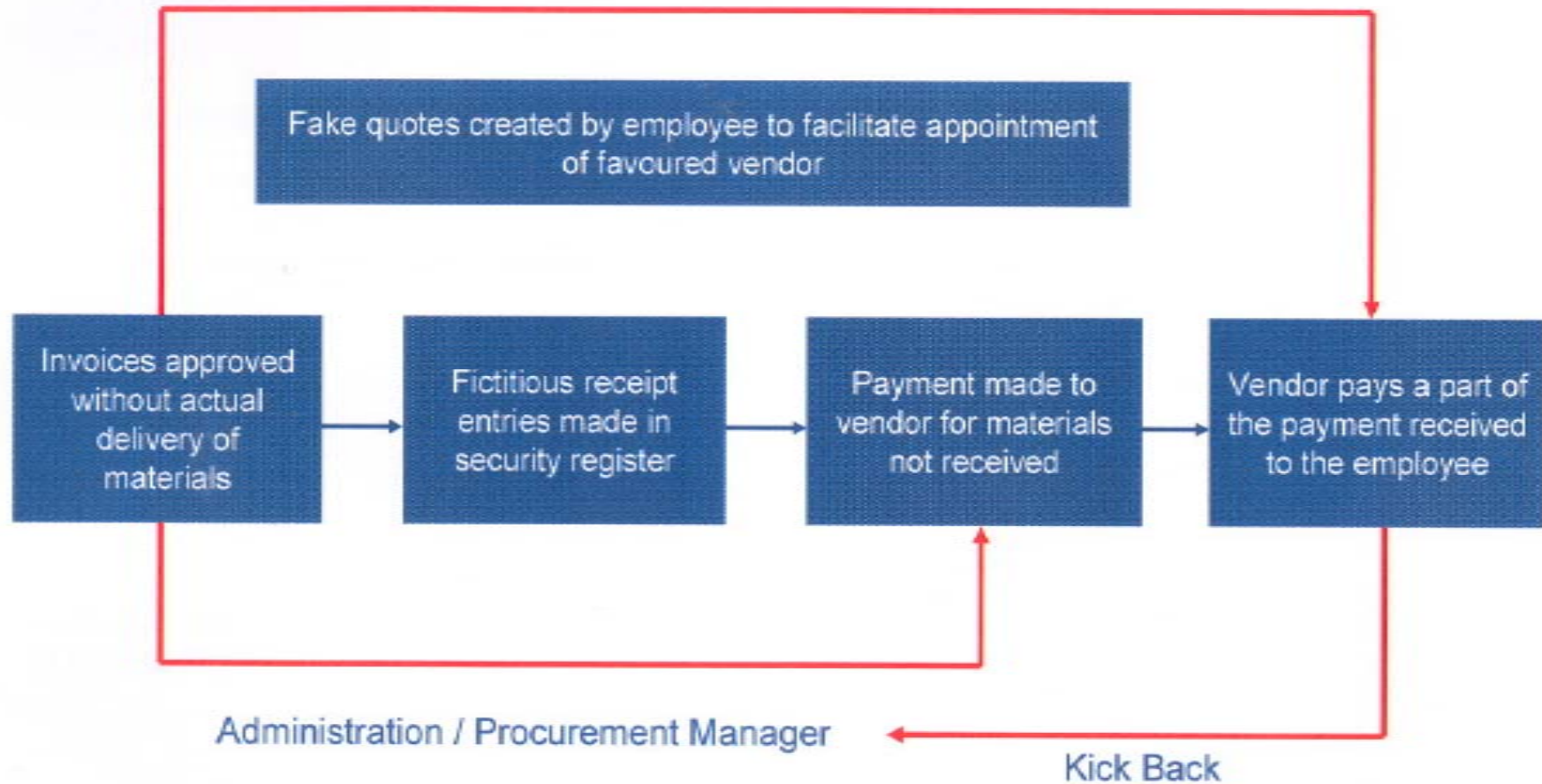
Thanking you,

With regards

For [Redacted] Service Station.



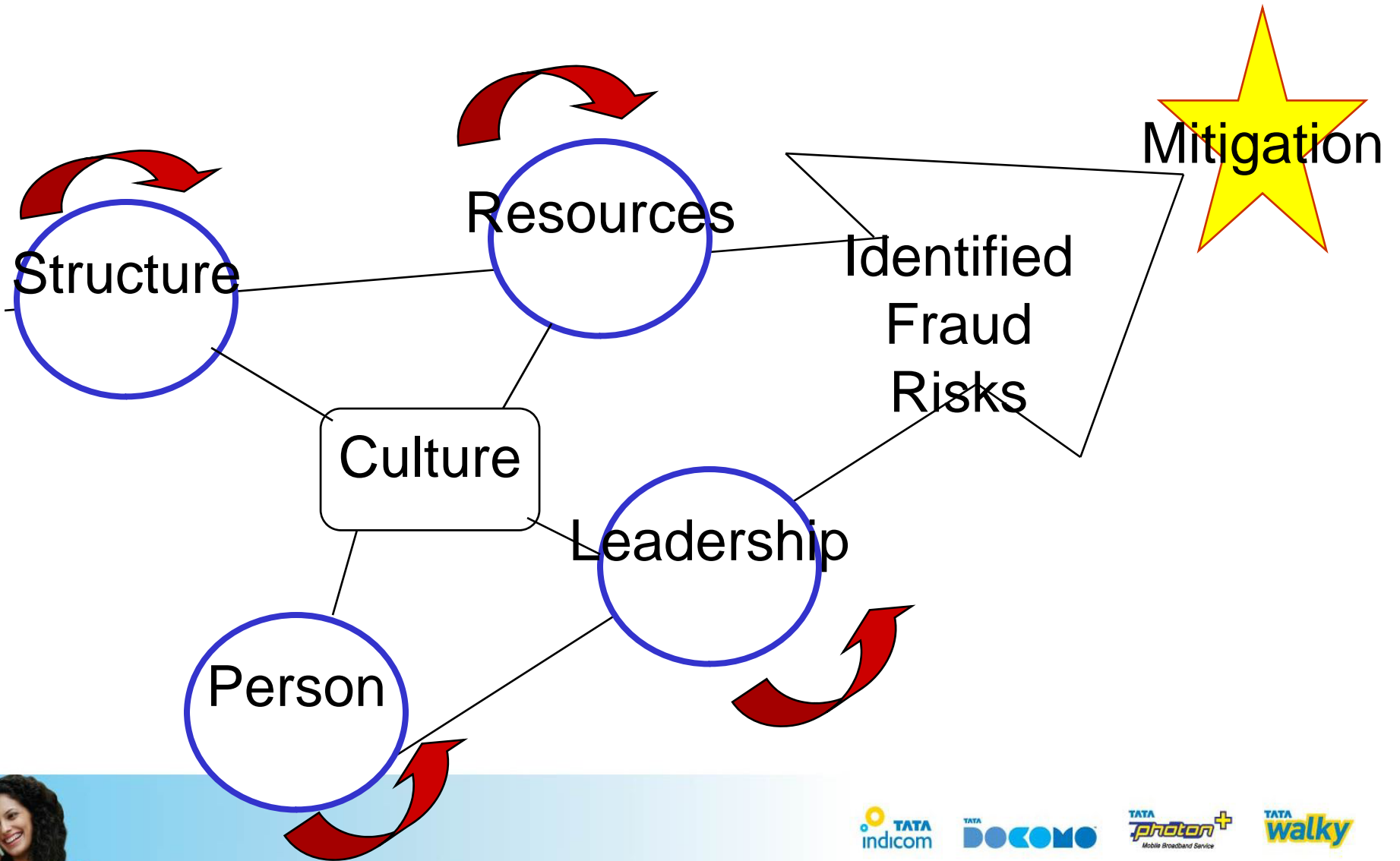
# Scenario 2 - Kickbacks to employees



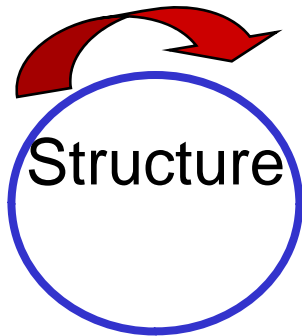
## Risk Mitigation



# Fraud Mitigation Strategies



# Alignment: Framework



- Org Structure
- Job Design
- Policies & procedures
- Governance, Internal Controls
- Management Systems, SOPs
- Central
- Special Task Force
- Internal Audit, Surprise Audit, Regular Audit (Surveillance)
- Levels of Authority



# Alignment: Framework



- Tools
- IT Systems
- Rules detection
- Whistle Blower
- Profiling/Assessment Tools
- Budget for Investigation, Litigation



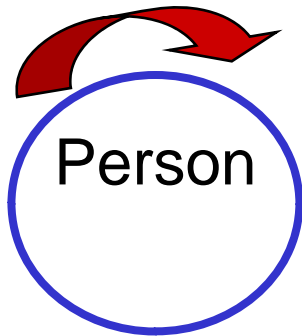
# Strategy: Framework



- Involuntary Role Modeling
- Personal accountability and Commitment
- Watch out: Current people promoted to Key Positions
- Promotional criteria



# Alignment: Framework



- New Employee Background checks
- Willingness to Punish
- Root Cause Analysis (Mager & Pipe)
- Rotation
- Fraud Detection & Analysis Competency
- High Risk Jobs
- IT breaches through Frontline



# The Four Desperates



1. Desperate  
Competition

2. Desperate  
Consumer

3. Desperate  
Achievers

4. Desperate  
Changes



# Possible General Root Causes for Fraud

1. "Everyone does it."
2. "It was small potatoes."
3. "They had it coming." – *the revenge syndrome*
4. "I had it coming." – *the equity syndrome*



# GENERAL STRATEGIES AND POLICIES

- Classification of Behaviors
  - Disrespectful Workplace Behavior
  - Progressive Discipline
  - Zero Tolerance
- Recruitment and Selection
- Exit
- Employee Assistance Program
- Anonymous Hotline
- Communication and Feedback
- Training and Education
- Formal Complaint and Grievance



# GENERAL STRATEGIES AND POLICIES

- Leadership
  - 1. Leaders act as role models whether consciously or unconsciously
  - 2. Leaders determine the working environment



# SPECIFIC STRATEGIES AND POLICIES

- **Theft and Fraud – Root Causes**

- Profile: 68.6% - no prior criminal record, Aged 26-40 years old, Annual income between RM15k-RM30k, 2-5 yrs of service
- Struggling financially or large purchases
  - difficult time in their lives
  - gets out of hand
- Merger and acquisition or reorganization activity.
  - ‘I don’t have a career here’ attitude.



# SPECIFIC STRATEGIES AND POLICIES

- **Theft and Fraud - Prevention**
  - Background checks
  - Duties segregated
  - Anonymous hotline
  - Communicate successes
  - Make a big noise when discovered
  - Video surveillance equipment



# SPECIFIC STRATEGIES AND POLICIES

- **Violation of confidentiality or security of company information – Prevention**
  - Security Policies
  - Ownership of Intellectual Property



# Employee related Red flags

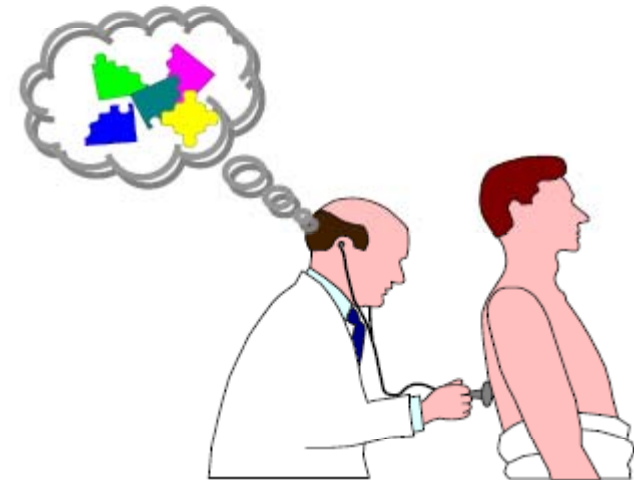


- ❑ Expensive lifestyle changes (Living beyond means)
- ❑ Behavioral changes: these may be indicative of drugs, alcohol and gambling
- ❑ Lack of job rotation in vulnerable areas
- ❑ Significant personal debt or credit problems
- ❑ Resistance to take vacations or sick leave
- ❑ “The only person that can do it” perception
- ❑ Explanations are quick but vague
  - ❑ Slow to provide proof
  - ❑ Easily annoyed at reasonable questioning
- ❑ Providing unreasonable responses to queries from Internal auditor, Finance, etc
- ❑ Over prepared for audit review
- ❑ Insist on dealing with supplier directly



# Qualities of an Effective FRAUD Analyst

- Unquestionable Integrity
- Highly Analytical
- Trainable and Knowledgeable
- Highly Motivated/Self-Starter
- Creative and Exploratory
- Flexible, Open to Diversity and Changes
- Systematic and Organized



# Summary

- No “Hard and Fast” Rule
- Highly Analyst Dependent
- Cannot be Fully-Automated
- Keep volume within Minimum levels
- Maximize all Data Sources
- Maintain Updated Reference Tables and
- Back-Up Records
- Detection is BEST esp. if done REAL-TIME
- Capitalize on Past Detections and
- Historical Records
- Careful and maintain Confidentiality

*Anticipate their moves –*

*“Think like a FRAUDSTER”*





**THANK YOU**

