The sources quoted in this presentation are only for academic research purpose for this private study group and not for commercial use.

For explaining concepts of fraud perpetration and its investigation, certain hypothetical scenarios have been constructed.

The cases referred to in this presentation are under investigation by various government agencies and at various stages of adjudication by various courts of law in India. The information presented in this study is sourced from news media and other websites on running an internet search. The case scenario being build may include fictional situations created only for better presentation of the concept.
## INDIA SURVEY

### Prevalence:
Companies affected by fraud

<table>
<thead>
<tr>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>69%</td>
<td>68%</td>
</tr>
</tbody>
</table>

### Areas of Frequent Loss:
Percentage of firms reporting loss to this type of fraud

<table>
<thead>
<tr>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft of physical assets or stock (33%)</td>
<td>Theft of physical assets or stock (27%)</td>
</tr>
<tr>
<td>Information theft, loss or attack (24%)</td>
<td>Information theft, loss or attack (23%)</td>
</tr>
<tr>
<td>Corruption and bribery (24%)</td>
<td>Internal financial fraud or theft (22%)</td>
</tr>
<tr>
<td>Internal financial fraud or theft (22%)</td>
<td>Corruption and bribery (20%)</td>
</tr>
<tr>
<td>Vendor, supplier or procurement fraud (20%)</td>
<td>Vendor, supplier or procurement fraud (20%)</td>
</tr>
<tr>
<td>Management conflict of interest (16%)</td>
<td>Management conflict of interest (16%)</td>
</tr>
<tr>
<td>Regulatory or compliance breach (16%)</td>
<td>Regulatory or compliance breach (16%)</td>
</tr>
</tbody>
</table>

### Increase in Exposure:
Companies where exposure to fraud has increased

<table>
<thead>
<tr>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>71%</td>
<td>67%</td>
</tr>
</tbody>
</table>

### Biggest Drivers of Increased Exposure:
Most widespread factor leading to greater fraud exposure and percentage of firms affected

<table>
<thead>
<tr>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT complexity (33%)</td>
<td>IT complexity (43%)</td>
</tr>
</tbody>
</table>

### Loss:
Average percentage of revenue lost to fraud

<table>
<thead>
<tr>
<th>2012-2013</th>
<th>2011-2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.4%</td>
<td>1.2%</td>
</tr>
</tbody>
</table>

Source: 2013/2014 Kroll Global Fraud Report
Although the growth in fraud for financial services this year was consistent with the experience of other sectors, it remains one of the most affected industries in 2012/13. With 75% of companies hit, the sector had the second highest overall incidence of fraud after manufacturing. Moreover, it had the most widespread problems in the survey with internal financial fraud (29%), regulatory or compliance breach (26%) and money laundering (8%). Although it saw a slight decline in the incidence of information theft – to 29%, from 30% in the previous survey – it still had the second highest frequency of this crime in the survey. Meanwhile, the rate at which financial services firms lost money to fraud (1.5% of revenue on average) is both above the median and more than twice the level found in the previous survey. Looking ahead, coping with complexity will be a major challenge for financial services companies. The sector has the highest number of respondents reporting increased fraud exposure from information technology (IT) complexity (47%) and from the ever greater complexity of its products (28%). High staff turnover is also cited increasingly as a driver of higher fraud risk (38%) in financial services than in any other sector, making dealing with complicated systems and offerings all the harder.

| Loss: Average percentage of revenue lost to fraud: 1.5% |
| Prevalence: Companies affected by fraud: 75% |
| Areas of Frequent Loss: Percentage of firms reporting loss to this type of fraud: Internal financial fraud or theft (29%) Information theft, loss or attack (29%) • Regulatory or compliance breach (26%) • Theft of physical assets or stock (23%) Management conflict of interest (20%) • Vendor, supplier or procurement fraud (18%) |
| Increase in Exposure: Companies where exposure to fraud has increased: 79% |
| Biggest Drivers of Increased Exposure: Most widespread factor leading to greater fraud exposure and percentage of firms affected: IT complexity (47%) |

Source: 2013/2014 Kroll Global Fraud Report
Which industries are at risk?

By industry, economic crime is most commonly reported in the financial services, retail and consumer, and communications sectors. Nearly 50% of respondents in each said they had been crime victims.
Processes under threat

Economic crimes threaten the basic processes common to all businesses – paying and collecting, buying and selling, growing and expanding, sourcing and supply chain.

procurement  distribution  supply chain
marketing  recruitment
onboarding  sales  international expansion
intellectual property  vendor selection
tax compliance  logistics
payments  data security

Source: PwC 2014 Global Economic Crime Survey
SCENARIO - 1
BRIBES & KICKBACKS
HR department observed that a certain officer in the Purchase department was resented by his colleagues and juniors as being arrogant and asocial.

Upon enquiries it was revealed that in last few years, some vendors with whom business was low were delivering to this particular officer sweets and gifts and sometimes for the entire department. Few of such suppliers were not in approved list with the company.

At annual HR review the employee was generally asked about his life and family where he proudly stated that his daughter stood first in her class. Interestingly the school he revealed was one of the expensive international schools in the city. Lifestyle improvements were also observed i.e., use of branded products, travel by radio taxi on daily basis for commuting, etc.

An inquiry into the matter was sought when at the annual Departmental Head meeting, the HR and Purchase Heads accidently discussed the employee in question at tea break, which was then escalated for approval by the management.
**BRIBES & KICKBACKS**

**RED FLAG INDICATORS**

- Disproportionate increase in wealth of the procurement official
- Frequent receipt of gifts
- Non-competitive selection of a contractor, unjustified favoritism.
Data collection IT: email backups, company mobile devices as per the company policy and applicable law, electronic data from the computer device of the suspect.

Data collection paper based: suppliers documentation since pre-vendor creation stage, quotes, bids, invoices, payments, delivery acknowledgements, revisions to contracts, etc. for the alleged suspects tenure with the company.

Data analytics will help identify relevant statistics - significant increase in business. Significant increase indicate most likely vendors who could have received business by paying kickbacks.
BRIBES & KICKBACKS

INVESTIGATION

Reviewing transactions thoroughly including bidding documents, order placements, contractual agreements, per unit prices, quality of goods and services, etc.

Background search on suspect vendors for their location, publicly available financial information via MCA or Financial database software's like Prowess or Capitalline, litigations against them, ownership structure, and overall market reputation.

Background search on the suspected procurement officer about his reputation in the department, increase in his assets, changes in his lifestyle, etc.
If significant indicators point towards fraud by the employee, asset trace investigation can be conducted to help recover the loss.

From data analytics, identification of vendors whose business has suddenly decreased or were removed from the approved list during this tenure needs to be identified. Informal discussions and discrete inquiries can be made with them. It is very likely that concrete information can come from such disgruntled vendors.

Combined analysis of data analytics, background checks, document reviews, discrete enquiries with vendors no longer being favored will give a good understanding of situation as to what is going on and who is involved.
SCENARIO - 2
COLLUSIVE BIDDING BY CONTRACTORS
A major infrastructure company had been awarded a road construction contract by the government under the PPP model.

For execution of the project, the company had sub-divided the geographies and execution areas and invited bids for the sub-contracting.

The company had publicized a whistle blower policy and received a complaint from one of the bidders about possible collusion between certain bidders.

The matter was sought to be investigated by the management of the company.
Winning bids too low when benchmarked against the company estimates, past experience and industry standards.

6 out of 10 bids shortlisted had very close price range, similar experience tenure, consistent in terms, conditions and technical specifications.

5 of these 6 operated from same commercial complex building with adjoining office numbers.

Some of the qualified bidders who failed to make it to short list were internally rated good for performance, based on past experience and their marked reputation.
COLLUSIVE BIDDING BY CONTRACTORS
INVESTIGATION

Prepare a questionnaire for interviewing the complainants and those who failed but rated good.

Interviewing complainants and confidential sources.

Data collection paper trail: bid documents, requests for bids, bid comparison documents prepared internally, Bill of Quantities (BoQs) comparison line item wise and bid securities.

Identify physical similarities in the bid documents like paper quality, colour schemes, type faces, formatting, language, etc.
COLLUSIVE BIDDING BY CONTRACTORS
INVESTIGATION

Connection between bidders on inter-company connections, common address, contact details, etc.

Unusual bidding patterns comparing the financial and quantity data line item wise. Test whether they are exact percentages or value apart.

Background check on all the final shortlisted bidders to check for common ownership, employees, affiliations or prior involvement in the other collusive bidding schemes.

Review the bid security details - whether issued by same bank branch to group of bidders, or issued to bidders by bank on same day.
Interview complainants and likely bidders who lost.

Most bid documents have a special enquiry / audit enabler clause. Exercising that right on the winning bidder is conducted as a routine formality. Instead, a detailed inquiry can be made into the business of the winning bidder.

Interviewing the winning bidder based on the information collected and collated from the above processes.
SCENARIO - 3
NSEL – FTIL CASE
Case study source: IOSR Journal of Business and Management www.iosrjournals.org, IES MCRC International Case Study Conference.

Creation of NSEL was ideated on concept that it would provide a platform for farmers to sell their produce and on the other hand processors, exporters, traders and investors to buy produce electronically.

This in theory would help price discovery in efficient way. NSEL was supposed to help the farmers to access the national market and get the best price for their commodities.

It was also envisaged that with the creation of holding capacity, the farmers would be able to raise funds under warehouse receipt financing by the banks.
Under Forward Contracts Regulation Act, a spot contract shall be settled within 11 days including payment and physical delivery of goods ie. in T+11 days.

Spot contracts are out of Forward Market Commission which is the regulatory authority.

Also as per Dept. of Consumer Affairs notification in 2007 the spot contracts were deemed to be out of FMC if settled in T+2 days.

NSEL some how managed to ensure ‘sell’ contracts at T+25 / T+35 and ‘buy’ at T+2 providing major players wide window for ‘arbitrage’.
Eventually, it was found that NSEL couldn’t honour their T+25/35 obligations as it neither had money nor commodities.

NSEL had also lent money to 24 borrowers without underlying commodity deposited by them – Warehouse receipt financing.

Exchange allowed trading in stocks without verifying existence of the same.

FMC found trading in contracts exceeding 11 days which was breach of provisions of FCRA, 1952. This led to unsettled payouts ballooning to Rs. 5400 crore.
**Facts of the Case**

It was found that the commodity stockists were selling warehouse receipts to investors for immediate payments.

The investors entered into buyback arrangements by selling back the commodity to stockists after 25-35 days without verifying the actual commodity stock.

These investors latter actually sold commodities without proof of underlying stock.

The NSEL scam has once again raised doubts over investing opportunities and investment safety.
How did central government allow NSEL to not follow demutualization rule?

Why there is no regulatory authority or monitoring mechanism for spot contracts in commodities?

Why were no red flags raised when liquidity was diminishing?

Why were no red flags raised when only few members of the exchange did the actual business for so many years?
Prepare a questionnaire for interviewing the complainants. Interviewing complainants and confidential sources.

Data collection paper trail: agreements between NSEL, brokers, stockists, brokers, contract notes, warehouse receipts, financial and non-financial records.

Data collection IT: email backups, electronic data from the computer device of all the suspects, server data, trade data, etc.

Connections between brokers, investors, warehouse owners, exchange shareholders on inter-company connections, common address, contact details, etc.
Data analytics: identify relevant statistics - significant increase in business of certain brokers, investors, warehouse owners, etc.

Data analytics: correlate the data based on trade time stamps, spurt in volumes, cartel of brokers, investors, warehouse owners, speculators, etc based on Time-Space Analysis.

Forensic analysis of financial records of the exchange, its holding company, brokers, investors, warehouse owners and all major traders in the exchange.

Specific focus on regulatory compliances and filings – both in terms of timely reporting and quality of the information reported.
SCENARIO - 4
DENA BANK – ORIENTAL BANK CASE
DENA BANK – ORIENTAL BANK CASE

FACTS OF THE CASE

Case study source: Various news paper reports

The fraudster posed as banker’s representative to various PSUs and Corporates for making fixed deposits with the bank.

PSUs and Corporates believed that they would be anyhow be dealing with the Bank and transactions would happen via regular banking channels, hence remain unsuspecting and trusting.

The fraudster would change his role when he visited the Banks and offered to bring huge deposits from companies. He acted as representative of PSUs and Corporates.
In OBC Case, upon transfer of Rs. 110 cr. by JNPT to the Bank for creating of FD, the fraudster asked the banker to immediately transfer the amount to his accomplice’s account Padmavati International via a FAX communication.

Immediately, that transfer was followed by another trench of Rs. 70 cr. for FD creation. The Bank again received instructions to transfer the amount to the accomplice’s account via FAX message.

Meanwhile, JNPT directly contacted Bank to enquire why FD Receipts were not yet delivered to the company. It was then, they and Bankers realised that fraud has been perpetrated on them.

The last trench of transfer was saved, but the earlier transfer of money is yet to be recovered.
In DB case, the Bank received bulk deposits from Corporates and PSUs between 30 January 2014 and 5 May 2014. The modus operandi was similar. The fraudster represented organizations and as banker to the other.

Fraudster convinced the organizations to create FD with the Bank and collected the KYC documents, obtaining signatures on forms, filled them and helped them through the entire process.

Fraudster then submitted forged documents with the Bank and obtained FDRs of Rs. 256.69 cr.

The originals were collected by the fraudster as representative of the organisations.
DENA BANK – ORIENTAL BANK CASE

FACTS OF THE CASE

The FDRs were subsequently pledged with the Bank by the ‘same signatories’ against which overdraft facilities of Rs. 223.25 cr were obtained.

The funds were then surreptitiously transferred out of bank. DB stock lost 5% and OBC stock lost 3.5% upon these revelations.

Bank FD scam gets bigger, 9 FIRs filed, estimated fraud atleast Rs. 700 cr. Preliminary inquiry by EOW currently on in another 10 cases.

Finance Ministry has ordered a forensic audit in these PSU Banks. Both the banks have complained to the CBI, which is also looking into the matter.
DENA BANK – ORIENTAL BANK CASE

RED FLAGS

MIDDLE MAN

Audience participation.....
DENA BANK – ORIENTAL BANK CASE

INVESTIGATION

In addition to the usual,
Document forensics: Paper and ink analysis, handwriting analysis, signature analysis.

Following regulatory channels, analyzing the email and telephone call data records.

Establishing the linkages between the fraudsters location while perpetrating fraud, communications with people within the organization and banks, etc.

Mapping the procedural role of banking officials and the PSUs-Corporates officials with their job description and the standard operating practices / rules governing their duties.
CONCLUSION

Defining safeguards is only the first step of fraud control process

Continuous risk reviews and adapting to changes in business environment will help in mitigating the fraud risks
“A Man who has never gone to school may steal from a freight car;

But if he has a university education, he may steal the whole railroad”

- Theodore Roosevelt
THANK YOU

For queries relating to the topic:
CA. Ajay R. Dave
Mobile: +91 9869252060
Email: ajay@ardassociates.in