

# Risk and Threat of Money Laundering Through Cybercrime

BKC - WIRC  
19th March 2016

# Major Cause



# Perception

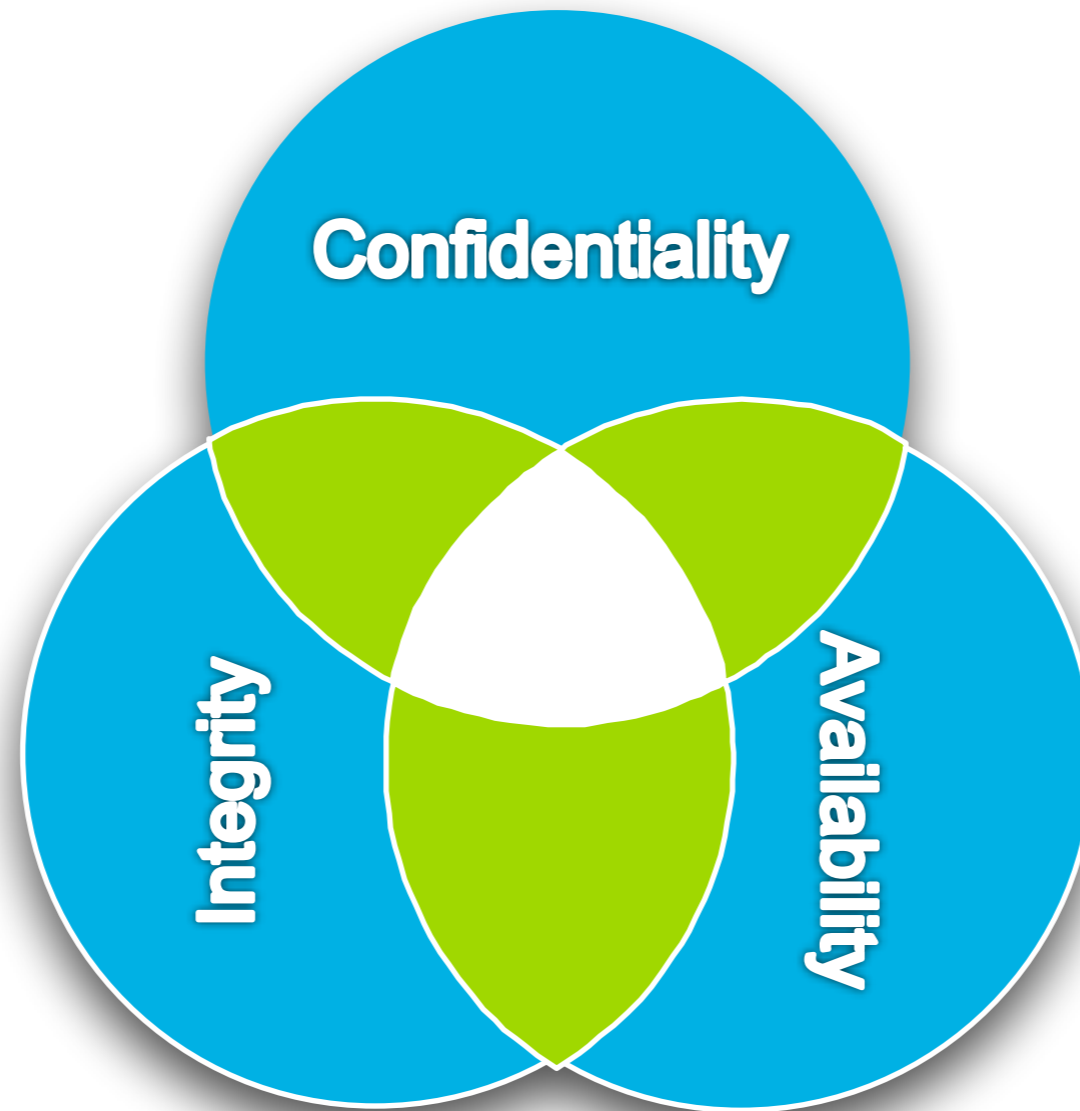
## Myth

- Converting Black Money to White is Money Laundering
- Money Laundering is done always by way of Big Scams
- Money Laundering is easy to do in certain types of businesses
- Anti Social Elements are majorily involved in money laundering
- Banks cannot stop money laundering

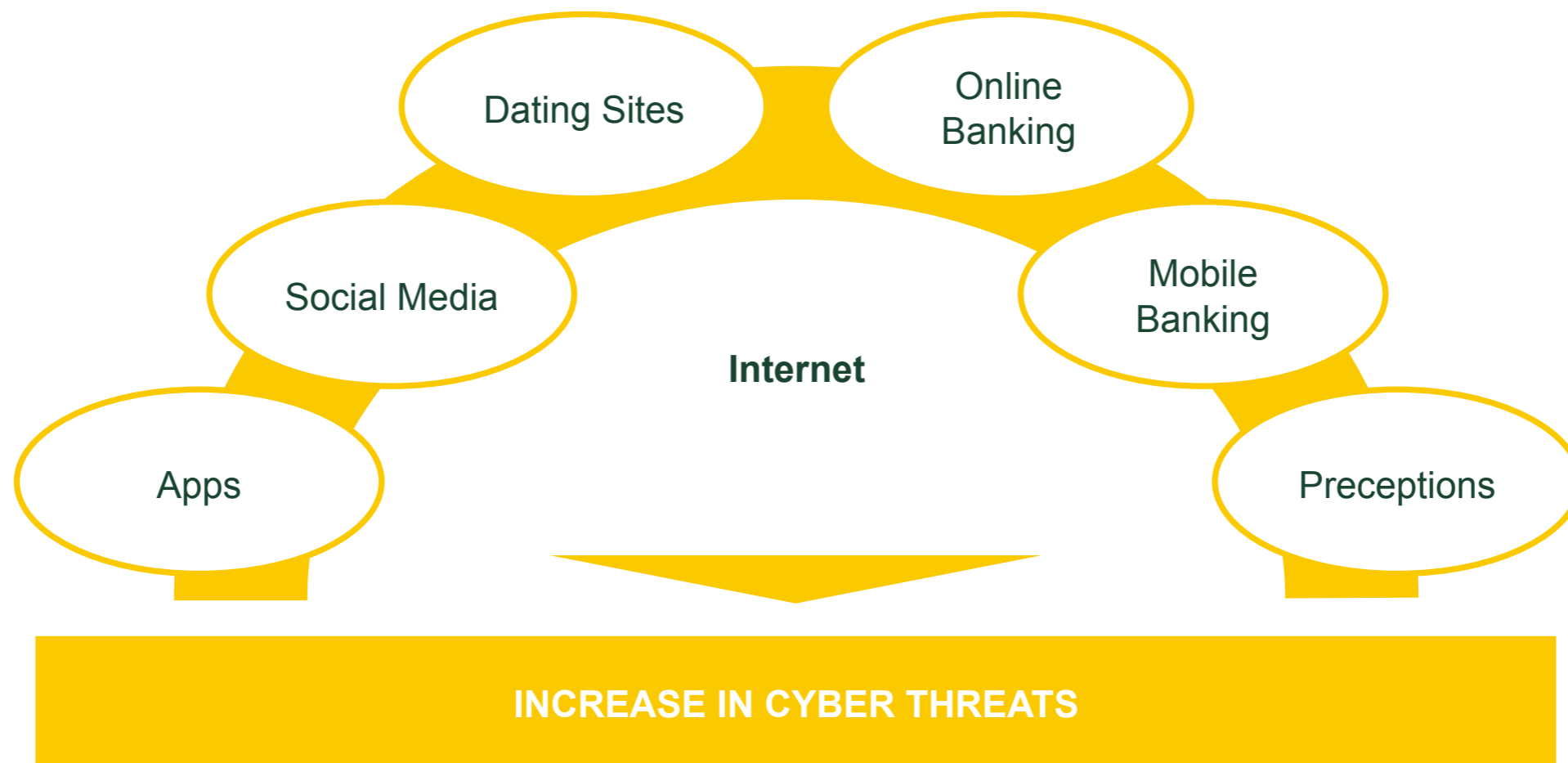
## Reality

- If someone conceals income to avoid Tax he will be tried under Income Tax Act and his action is not considered money laundering
- Businessmen are involved in money laundering in a big way
- Bank of Baroda Scam – Collusion and Lapse in monitoring lead to consequences

# Cybercrime Targets



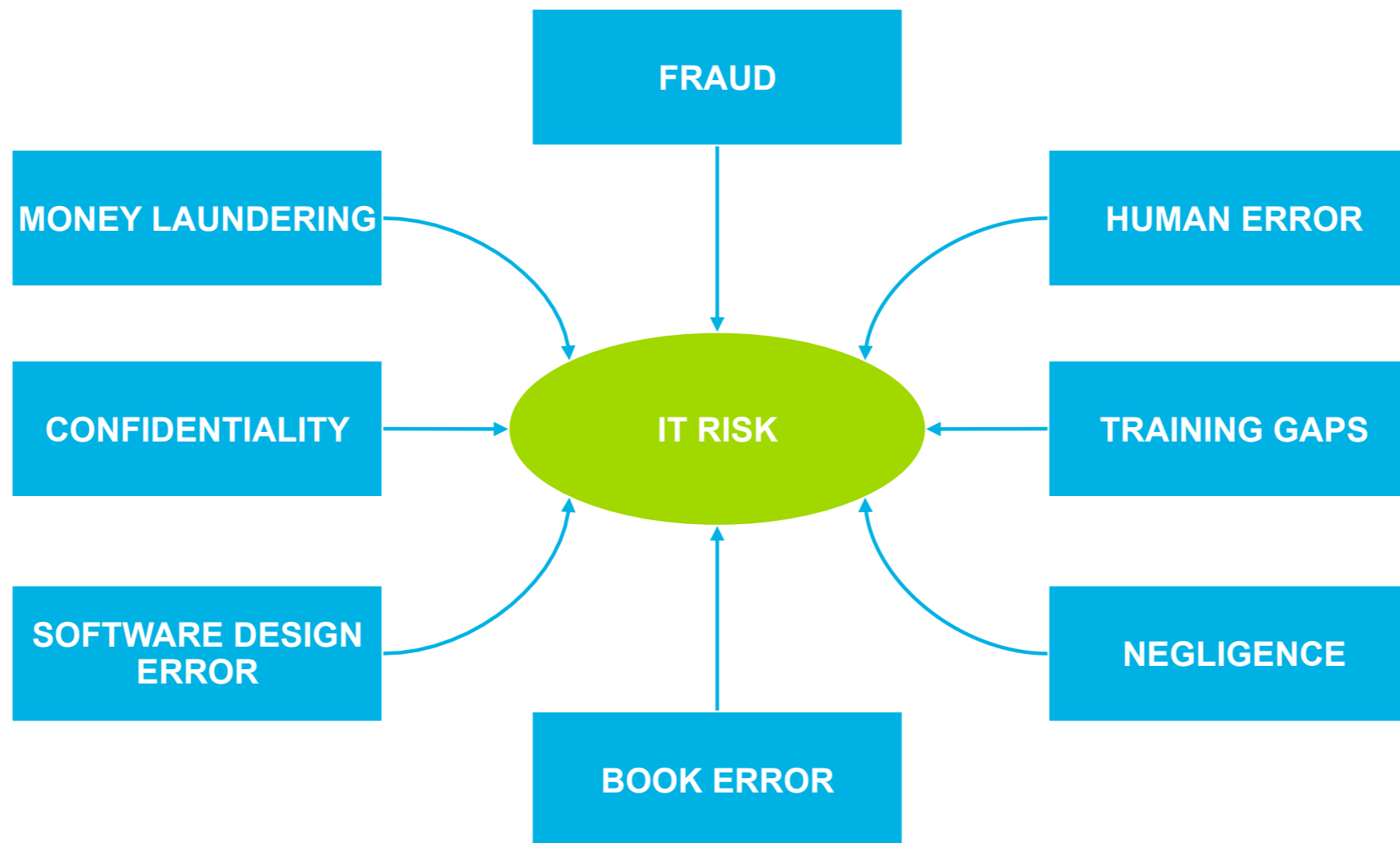
# Cause



# Effects

- Reputation Loss
- Weakens Competitiveness in democratic institutions in society
- Destabilises Economy
- Impetus to Criminal Activities
- Discourages outside investment
- Encourages tax evasion culture

# IT - Challenges



# Indian Scenario

- Out of 140 countries, India has been ranked 93rd and 70th in 2012 and 2013 respectively with a score of 6.05 in 2012 and 5.95 in 2013, as compared to Norway, which has a score of 2.36 and ranks No. 1 in the Anti Money Laundering (AML) Basel Index 2013. AML Basel index is country risk ranking which focuses on money laundering / terrorist financing risk, consisting of 14 indicators of assessment.
- This clearly shows that India, in the present-day scenario, is very vulnerable to money laundering activities and is a high risk zone.
- India needs to curb Money laundering as the practice is rampant across the country. It is estimated that a total of \$343 billion has been laundered out of India during the period 2002-2011. This is a massive amount and prevention of money laundering must be a priority for the government!
- Initiatives - PMLA 2002; PMLA 2012, PMLA Rules 2013; Black Money Act ; FIU India
- Other anti-money laundering regulators in India include:
  - Securities and Exchange Board of India (SEBI)
  - Reserve Bank of India (RBI)
  - Insurance Regulatory & Development Authority of India (IRDA)
  - Directorate of Enforcement, Central Bureau of Investigation – Economics Offences Wing
  - Income Tax Department



# State of Affairs

- \$2 trillion The sum laundered globally, according to the United Nations Office on Drugs and Crime (UNODC). This is about 3% of the world GDP.
- NEED FOR BANKS TO COMPLY - According to Prevention of Money Laundering Act (PMLA), the director of FIU-IND can impose fines on banks and other financial institutions if they fail to detect or conceal wrongdoings
- INVESTIGATING AUTHORITIES
- The Enforcement Directorate carries out investigations. The ED is also empowered to attach property of entities involved in money laundering. The investigation begins with filing an Enforcement Case Information Report (ECIR), which is comparable with an FIR.
- The Adjudicating Authority under PMLA then decides whether the attachment is valid or not. The courts take the final call on punishment and confiscation of property from the money launderers.
- PENALTIES AND PUNISHMENT - Rigorous imprisonment of no less than 3 years and up to 7 years. The PMLA Amendment Bill which is currently in Parliament has proposed that the jail term should go up to 10 years.

# Some Sparks



ED has summoned Vijay Mallya to record his statement in the case. (photo TOI)

**M**UMBAI: The Enforcement Directorate (ED) is learnt to have got a couple of crucial leads while examining bank documents in the Rs 900-crore money laundering case connected with the defunct Kingfisher Airlines (KFA) case. Officials said that they manage to get the leads while examining a complex bank transaction.

## Prominent Money Laundering Cases



**₹223Cr**

Kalaignar TV (DMK first family)



**₹202Cr**

Satyam Computers' founder  
B Ramalinga Raju



**₹168Cr**

Former minister of Jharkhand  
Anosh Ekka



**₹112Cr**

Former CM of Jharkhand  
Madhu Koda

**बैंक ऑफ़ बड़ौदा**  
**Bank of Baroda**  
India's International Bank

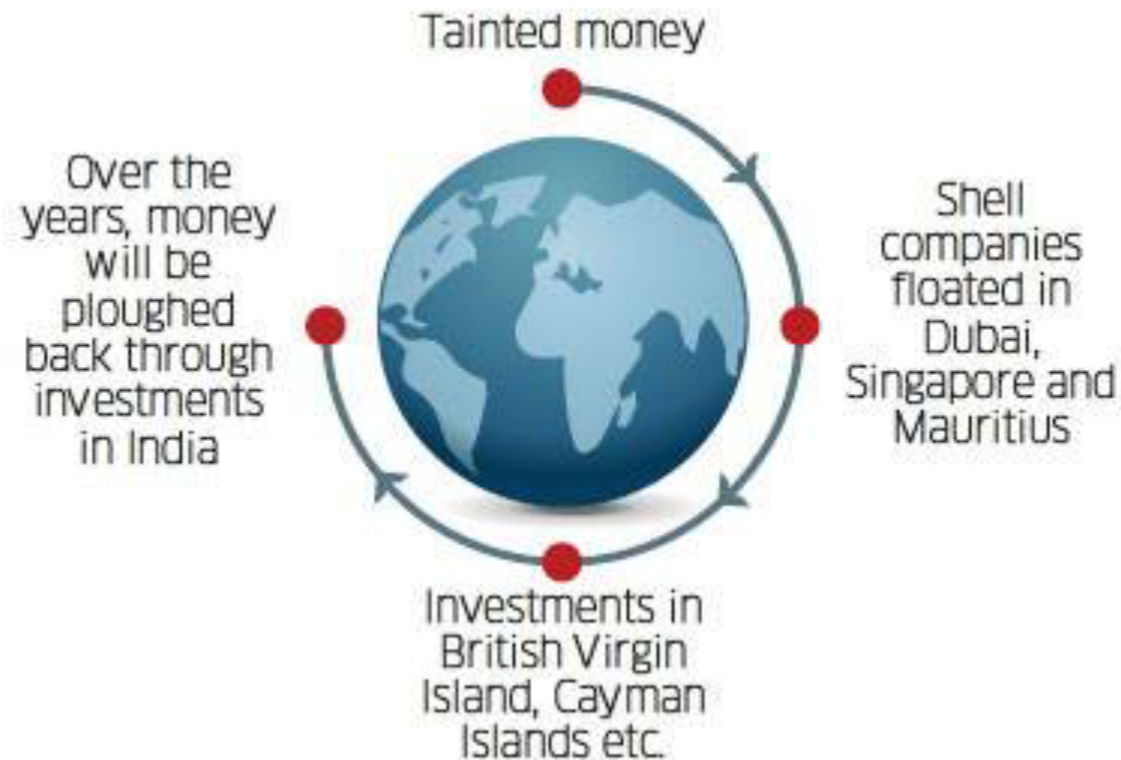
Six Arrested in Bank of Baroda's Rs 6000 Crore Money Laundering Case

NEW DELHI: Six persons have been arrested in the case involving alleged laundering of black money to the tune of ₹ 6000 crore at a branch of Bank of Baroda.

# Modus Operandi

## *How it Works?*

Indian Investigators tracking scams such as 2G, Commonwealth Games and Madhu Koda suspect the following as the favourite route for shifting ill-gotten money



Thanks to the banking system, the travel time of millions of dollars across a few continents is just a few hours. But to recover the same, India has to go through legal processes including inking of treaties with each country.

# Snippets.. (as of 2013)

- 1437 Total number of money laundering cases registered in the country for investigation
- 131 :Total number of cases where attachment of property is confirmed
- Rs. 1214 crore : worth of properties attached so far
- Rs. 30 Lakh : Minimum threshold limit for tainted money for a money laundering case to be filed. Exceptions are serious crimes like terrorism and narcotics
- 22 : No of persons arrested in India in money laundering cases
- 30 : No of Acts, violation of which attracts money laundering cases

# Cybercrime Variants

- Cyber Stalking
- Hacking
- Phishing
- Cross Site Scripting
- Vishing
- SPAM
- Vulnerability
- Wealth Managers
- Investment Advisors
- Shell Companies
- Single Shareholder Companies
- Offshore Trusts



# India joins the battle

## *India Joins Battle Against Money Laundering*

India joined as 34th member of Financial Action Task Force (FATF) in June 2010. This is expected to help India trace terror funds and prosecute money laundering offences

India joined the Asia Pacific Group (APG) against money laundering. Kochi hosted its annual meet in 2011.

India gained membership of Eurasian Group (EAG) in December 2010.

New Delhi joined Egmont Group in 2007. The group is a network of Financial Intelligence Units (FIUs) across the world.

# Black Money Act

- Introduced in March 2015
- The Act provides for separate taxation any undisclosed income in relation to Foreign Income and Assets
- Such income will be taxed under the stringent provision of this Act

# Online Money Laundering

- Emergence of electronic money and global systems of electronic payment formed a parallel banking system
- It allows one to rapidly transfer funds to any country anonymously through tangled routes
- Hence being used as one of the most effective tools to launder illegal money, conceal income to evade taxes.
- It plays a fundamental role in facilitating the ambitions of people who need to avoid the attention of authorities that sudden wealth brings from illegal activities



# Extent and Method

- Estimates of the size of the money laundering problem ranges between \$590 billion - \$1.5 trillion annually. This is a staggering amount and detrimental by any calculation to the financial systems involved
- Many small time software companies are known to be the front to carry out money laundering activities
- Methods used
  - ○ Placement
    - Cash paid into bank (sometimes with staff complicity or mixed with proceeds of legitimate business)  
Cash used to buy high value goods, property or business assets.
  - ○ Layering
    - Wire transfers abroad (often using shell companies or funds disguised as proceeds of legitimate business)  
Cash deposited in overseas banking system
  - ○ Integration
    - False loan repayments or forged invoices used as cover for laundered money  
Income from property or legitimate business assets appears "clean".

# Case Study - 1

In a small branch of big bank advances shot up 100% in a particular year. Loan portfolio contained bill discounted.

The perpetrator of the fraud in collusion with the branch manager opened 36 different Inland Letter of Credit and Bill discounted. The bills were raised on one party by other and circular reference was never completed. Every company had different management but the fraud was unearthed when the Demand Draft of three parties was collected by a single person

# Case - II

The Bidhannagar Police's cyber cell arrested an employee of Wipro after the tech MNC lodged a complaint against unknown persons stealing sensitive data. This is the second arrest based on a specific complaint by the firm.

- Calling it a case of trade-based money laundering, where accused traders evade custom duties and taxes to generate slush funds, the agency arrested Kamal Kalra, working with the foreign exchange division of HDFC bank, Chandan Bhatia, Gurucharan Singh Dhawan and Sanjay Aggarwal after marathon questioning at its office here.
- Emails sent to HDFC bank for its reaction did not elicit a response.
- All the accused, ED sources said, were alleged middlemen for at least 15 fake companies, out of the total 59 which were involved in the perpetrating of the economic crime unearthed recently and also being probed by the CBI.
- Sources said the four allegedly connived with each other in “forming” fake companies and business entities in Hong Kong by “over valuing” the export value and subsequently claiming duty drawbacks.
- While ED investigations under the Prevention of Money Laundering Act (PMLA) claimed that the HDFC employee was allegedly helping Bhatia and Aggarwal for remitting the amount through BoB against a commission of 30-50 paise per US dollar remitted abroad, Bhatia was allegedly instrumental in forming the companies in India and used to remit money to companies based at Hong Kong and was working with Dhawan, an exporter of readymade garments.
- They alleged Aggarwal was successful in sending tainted foreign remittances worth Rs 430 crore through the BoB branch in Ashok Vihar in a short span of time.
- Sources said more arrests of similar middlemen and other operatives, including BoB employees, could take place in the near future.
- The agency is also probing the case for forex contraventions under the Foreign Exchange Management Act (FEMA).
- The agency said BoB yesterday informed it that “the total amount deposited in the 59 accounts is Rs 5,151 crore and only 6.66 per cent (Rs 343 crore) of this amount has been deposited in cash in the bank while remaining amount of Rs 4,808 crore came through other banking channels.”

# Challenges

- Lack of technical expertise and equipment hamper the investigation of cyber crime cases in the Port City along with the delay in getting the information from the different service providers.

# Scary but true

- According to a report by Akamai Technologies, an internet content delivery network, India is ranked eighth in the world in terms of origin of attacks.
- There are underground forums where people post their hacking requirements and hackers bidding for it. The money will be transferred to a PayPal account via a service called Perfect Money. It is type of an e-currency which can be transferred between customers, whose identities can be hidden and it can be redeemed for cash, in Dollars or Euros. One can access the hacker forums only through Tor Browser that allows access to the 'hidden web' where these black hat-hackers operate.
- In June, there was a sophisticated and extensive cyber espionage attack that emanated from India which targeted Pakistan based government bodies among other anti-national forces. According to Norway based security firm Norman, the attacks that continued for four years have been named as "Operation Hangover." The report says that the primary goal of the group is to gather intelligence from a combination of national security targets and private sector companies.

# BOrDerleSS CriMe

- Think of the internet as a system or network of connections within which organized crime groups thrive. In the past, criminals were fairly indigenous to the towns and cities where they lived. They learned their trade in their immediate environment and very often be sent to prison where they would meet criminals with different skills and abilities. Once released, many would commit further crimes and stay in touch with those still behind bars, often on a national basis. Sometimes, very occasionally and particularly in the drugs war, criminals were able to cross territories and boundaries.
- That has all changed. With internet access, a criminal based in a at in london can commit a crime in, for example, Shanghai. The internet has made it easy for organized crime groups to commit crimes across borders, taking advantage of the obstacles which law enforcement of cials encounter when trying to work across international boundaries.

N K Bhat & Co

---

Chartered Accountants