### CA - FINAL RISK MANAGEMENT

<table>
<thead>
<tr>
<th>Name</th>
<th>Particulars</th>
<th>Particulars</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Bank of Baroda’s</td>
<td>The Financial Intelligence Unit (FIU) has slapped Rs 9 crore penalty on Bank of Baroda for &quot;failing&quot; to adhere to anti-money laundering norms, and not having an effective system to report suspicious transactions linked to the Rs 6,000 crore scam in its Delhi-based branch. The FIU has levied the maximum penalty of Rs 1 lakh, as stipulated under the Prevention of Money Laundering Act (PMLA), for each instance of &quot;delayed&quot; filing of Suspicious Transaction Reports (STRs) by the state-owned bank in the case. After about three years of investigation, the FIU has held that the bank failed on at least five counts in detecting wrongdoing and instances of money laundering at its branch in Ashok Vihar in Delhi, where a Rs 6,000 crore forex remittance scam had been reported in 2015. The FIU said the bank failed to have effective internal system in place for disposal of 8,692 alerts, detecting and reporting suspicious transactions, failure in carrying out effective customer due diligence in</td>
<td>1. It was alleged that a whopping Rs 6,172 crore black money was remitted from Bank of Baroda to Hong Kong camouflaged as payments for non-existent imports like cashew, pulses and rice. The amount was allegedly deposited in 59 accounts in cash as advance for imports that never existed. On October 12, 2015, CBI and the Enforcement Directorate started investigating the matter. 2. It is also alleged that the amount was deposited in 59 accounts of the bank’s Ashok Vihar branch (New Delhi) in cash as advance for import and the money was sent to some select companies in Hong Kong. 3. The branch opened 59 current accounts from May 2014 to June 2015 through which large foreign exchange remittances were made, the Bank of Baroda said in a regulatory filing. 4. During this one year, a total of 5,853 outward foreign remittances aggregating USD 546.10 million (around Rs 3,500 crore) were made through 38 current accounts to various overseas parties numbering some 400, mainly based in Hong Kong and one in the UAE. 5. Remittances were sent to Hong Kong and Dubai via banks, actual exports were sent to Afghanistan. “The records show that the alleged exports were sent to Afghanistan but invoices were generated by Hong Kong importers. It is now a matter investigation as to who</td>
</tr>
</tbody>
</table>
respect of 73 accounts, delayed filing of 8,822 EFT (electronic funds transfer) reports and failure to file EFT reports in respect of transactions in two separate accounts. The FIU rued that despite large number of cash transaction reports in respect of four newly opened bank accounts belonging to one family, none of them were converted into STRs (suspicious transaction reports).

6. Much before 59 accounts, which are under the scanner of the ED and the CBI, were opened in Bank of Baroda, 13 accounts were opened in HDFC Bank during February-March 2015 to send money abroad.

7. Reacting to the developments, an HDFC Bank statement said: “The matter is being examined internally on top priority. The bank is also extending its full cooperation and support to the authorities. The bank has a zero-tolerance policy for any misconduct on the part of its staff.”

8. P S Jayakumar, the former chief executive of VBHC Value Homes took charge as the new MD and CEO of the of the scam-hit Bank of Baroda for three years on October 13, 2015. BoB had remained headless for the past 14 months.

9. Finance Minister Arun Jaitley said the magnitude of the alleged black money transfer through state-owned Bank of Baroda (BoB) will only be known after completion of the multi-disciplinary probe.

10. On October 12 as many as six persons, including Garg and Dubey were arrested on charges of criminal conspiracy, cheating and provisions of the Prevention of Corruption Act. The other four arrested, include Kamal Kalra, working with the foreign exchange division of HDFC bank, Chandan Bhatia, Gurucharan Singh Dhawan and Sanjay Aggarwal.
2. **Punjab National Bank (PNB) allegedly committed by diamantaire Nirav Modi and his uncle Mehul Choksi, the promoter of Gitanjali Gems.**

On 14th Feb 2018, PNB noticed fraudulent transactions worth Rs 11,346 crore at one of its branches in Mumbai. Apparently the branch staff issued fake LoU (Letter of understanding) for buyer’s credit to companies of Nirav Modi and Gitanjali Group. Companies like Gitanjali Gems, Gili India, Nakshatra and Nirav Modi are said to be involved in this scam.

PNB says that on 16 January the accused firms presented a set of import documents to the Mumbai branch and requested buyers’ credit to pay overseas suppliers. Since they had no pre-arranged credit limit, the branch official asked the companies to put down the full amount as collateral so the bank could issue LOUs to authorize the credit.

When the firms argued that they had used such facilities in the past without keeping any money on margin, PNB scanned through records and found no trace of any transactions, according to the bank’s account. It then found that two junior employees had issued LOUs on the SWIFT interbank messaging system without entering the transactions on the bank’s own system. Such transactions went on for years without detection, PNB said.

Banking sources have said in some banks the SWIFT system, which is used for international transactions, and the core banking system work independently of each other. In PNB’s case, it said the outstanding LOUs were not available on its core banking system run on Infosys’s Finacle software. Thus the LoUs issued went undetected.

3. **Rs 400-cr fraud at Citibank branch**

A banking fraud which could run into a whopping Rs 400 crore has been unearthed at leading multinational lender Citibank's Gurgaon (Haryana) branch. Gurgaon Police Commissioner SS Deswal said an FIR under sections of cheating and forgery against a bank employee and three others has been lodged and 18 accounts having close to Rs 4 crore have been frozen. Sources said funds amounting to Rs 400 crore of 20 high networth customers has been siphoned off. The fraud is said to be a handiwork of Shivraj Puri, the employee who is alleged to have sold investment products to high networth clients, claiming that they would generate unusually high returns. It is also alleged that Puri, who is named in the FIR, showed a forged notification of market regulator Securities and Exchange Board of India for obtaining funds from customers. He is also accused of claiming that these products were authorised by the bank's investment product committee. The bank in a statement said, "We immediately reported the matter to all the relevant regulatory and law enforcement authorities. Identified suspicious transactions have been isolated and we are providing full assistance to the authorities in their investigations." Sources said Puri allegedly sought deposits from high networth customers in lucrative schemes but...
transferred the funds to some fictitious accounts. Funds amounting to Rs 400 crore belonging to about 20 customers were transferred to such accounts, they said. "We recently initiated an investigation into a certain set of suspicious transactions based on documents forged by an employee involving a few accounts in our Gurgaon branch," the bank statement said. The bank said the issue did not impact other accounts or transactions or customers of the bank.

4. Bank Scam by Vijay Mallya

Mallya's Kingfisher Airlines had borrowed Rs 9,432 crore from 13 banks till February 2018. The State Bank of India was the biggest lender with 1600 cr. followed by the PNB 800 cr, IDBI 650 cr and Bank of Baroda lend 550 cr. Mallya left India on March 2, 2016 and hiding in the London and the government of India is fighting for his extradition till date.

5. R P Info Systems Bank Scam:

The CBI has booked a computer manufacturer R P Info Systems and its directors for allegedly cheating a consortium of 9 banks with amount of Rs. 515.15 crore. This company has used fraud documents to take the loan. CBI had raided the offices of the company in Kolkata and other places on February 28, 2018.

6. First Leasing Company of India Limited (FLCL)

FLCL was the first Indian leasing company incorporated in September 1973 and commenced its operations in India from November 1973 in Madras. It came out with its first public issue in 1983 under the promoter ship of A C Muthiah and Farouk Irani. The former was the Chairman and the latter was its Managing Director. Since the company was a Non Banking Financial Institution (NBFC), it had a great market demand for leasing and hire-purchase transactions Farouk Irani, the Managing Director of the First Leasing Company Limited admitted the fraud in 2013 which it led for several years along with the Industrialist AC Muthiah, have declared that the balance sheets are manipulated to the extent of Rs. 1000 crores. There was a falsification of balance sheet, by overstating the accounts payables, etc. on the liability side with creation of some non-existence asset on the asset side of the balance sheet. The Managing director of the Company started diverting the company’s assets in the name of his relatives, close associates and himself. When the bankers had asked the company to pay its loan it said it does have enough funds to re-pay, rather it declared that its assets are insufficient to re-pay its liabilities.

7. 3.2 million debit cards compromised; SBI, HDFC Bank, ICICI, YES Bank and Axis worst hit

About 30 lakh bank debit cards have come under threat after a security breach at a private bank's ATM raised fears of potential fraud, according to media reports. Though this is just about half a percent of total cards issued in the country, this could be the biggest security breach in the Indian banking industry, say reports. However, banks have advised customers to not panic as they are taking steps to prevent any major trouble. According to media reports, the payment systems of Hitachi Payment Services were infested with malware that helped miscreants to steal personal information and do fraudulent transactions. The breach might have happened at YES Bank as Hitachi manages the bank's ATMs, says a report in
The Times of India. The reason why other banks became vulnerable is because YES Bank ATMs see many third party transactions, says the report. What is worrisome is that the breach was effected in such a way that anyone using the bank's ATMs in the region would risk having data compromised, a PTI report said citing bankers. "Data processes of one private bank was compromised which affected other banks' customers well. Customers who used that bank's ATM stand to get potentially affected," the PTI report quoted a banker as saying without naming the bank. Though the bankers claim the breach has not led to any monetary losses to anyone, the ET report says some customers have complained of unauthorized usage from China. YES Bank on its part has "proactively undertaken a comprehensive audit of ATMs". "There is no evidence of a breach or compromise on ATMs. We continue to work with relevant stakeholders, including other public sector and private banks, and NPCI, to ensure utmost safety and security of ATM network and payment services which are completely safe to use," a bank spokesperson told the PTI. Hitachi too has denied that its systems have been compromised. "I do not think it is necessary for any bank to reissue cards," Loney Antony, MD, Hitachi Payment Services, has been quoted as saying in the ToI report. With online bank frauds on the rise, the RBI had recently proposed that a customer will not be liable to make the payment if the fraud or negligence is on part of the bank and the customer notifies the lender within three working days of receiving communication from the bank regarding unauthorised transaction by a third party. If the customer's own involvement is not clearly established, customer liability will be limited to a maximum of Rs 5,000 if he reports within 4 to 7 working days. A customer's entitlement to zero liability shall arise where the security architecture and systems of the bank for electronic banking transactions are not able to protect the customer for fraud/ negligence on the part of the bank, the RBI said in its draft norms in August 2016.

8. Airtel Payments Bank Ltd

Airtel Payments Bank Ltd has received requisite approvals from the Reserve Bank of India (RBI) and the Unique Identification Authority of India (UIDAI) to start onboarding customers using Aadhaar based e-KYC (know your customer), the bank said on Thursday. This comes as a big relief to the bank which has not been able to enrol customers since January. "We thank the authorities for the approvals. We remain committed to the government’s vision of financial inclusion and banking for all,” said a spokesperson of the bank. In December last year, the UIDAI had temporarily suspended Airtel and its payments bank from conducting Aadhaar-based verification of its mobile customers as well as those of the bank using the e-KYC process after receiving complaints that it was opening payments bank accounts without the explicit consent of users. It was also alleged that government subsidies were being credited in these accounts without the knowledge of users. The telco had deposited ₹2.5 crore as penalty
with the UIDAI. It also credited back ₹138 crore of funds under the direct benefit transfer scheme to the original accounts of 5.6 million beneficiaries. Following this, the UIDAI decided to conditionally allow Bharti Airtel Ltd to resume Aadhaar-based e-KYC verification of telecom subscribers. However, the suspension of the e-KYC licence of Airtel Payments Bank was not revoked. In January, RBI directed the bank not to onboard new customers. In March, RBI also imposed a penalty of ₹5 crore on the bank for violating operating guidelines and KYC norms. The fine was imposed after RBI scrutinized the bank’s documents relating to the opening of accounts without specific or clear consent from the customers. Airtel Payments Bank had denied any wrongdoing and streamlined its processes to comply with the regulations. Airtel Payments Bank was the first payments bank to start operations on 12 January last year with an investment of ₹3,000 crore. Other payments banks that have started operations are India Post Payments Bank Ltd, Paytm Payments Bank Ltd, Fino Payments Bank Ltd, Aditya Birla Idea Payments Bank and Jio Payments Bank. Payments bank is a differentiated bank providing a limited range of products, such as acceptance of demand deposits and remittances of funds. It can accept a restricted deposit, which is currently limited to 1 lakh per customer. However, these banks cannot issue loans and credit cards.

| 9. Sterlite Copper plant to shut down permanently |
| Sterlite Copper plant at Thoothukudi will be sealed permanently, says a Government Order issued by Environment and Forests department. This follows directions issued by Tamil Nadu Pollution Control Board (TNPCB) for closure and disconnection of power supply to the unit last week. The Government Order said, it is brought to the notice of the Government that TNPCB did not renew the Consent to Operate to Vedanta Limited, Copper Smelter Plant in its order on April 19, 2018. Subsequently on May 23, TNPCB issued directions for closure and disconnection of power supply to the unit. The power supply has been disconnected on May 24. Under Sections 8(1)(b) of the Water Act, 1974, in the larger public interest, the Government endorse the closure direction of the TNPCB and also direct the TNPCB to seal the unit and close the plant permanently, says the order issued by Md Nasimmuddin, Principal Secretary to Government. The Deputy Chief Minister, O Panneerselvam, has asserted that the government will take resolute steps for the permanent closure of Vedanta group’s copper plant here. |
As per RBI Circular:

Early Warning Signals (EWS)

Some Early Warning Signals (EWS) which should alert the bank officials about some wrongdoings in the loan accounts which may turn out to be fraudulent

1. 
   a. Default in undisputed payment to the statutory bodies as declared in the Annual report.
   b. Bouncing of high value cheques
2. Frequent change in the scope of the project to be undertaken by the borrower
3. Foreign bills remaining outstanding with the bank for a long time and tendency for bills to remain overdue.
4. Delay observed in payment of outstanding dues.
5. Frequent invocation of BGs and devolvement of LCs.
6. Under insured or over insured inventory.
7. Invoices devoid of TAN and other details.
8. Dispute on title of collateral securities.
9. Funds coming from other banks to liquidate the outstanding loan amount unless in normal course.
10. In merchanting trade, import leg not revealed to the bank.
11. Request received from the borrower to postpone the inspection of the godown for flimsy reasons.
12. Funding of the interest by sanctioning additional facilities.
13. Exclusive collateral charged to a number of lenders without NOC of existing charge holders.
14. Concealment of certain vital documents like master agreement, insurance coverage.
15. Floating front / associate companies by investing borrowed money
17. Liabilities appearing in ROC search report, not reported by the borrower in its annual report
18. Frequent request for general purpose loans.
19. Frequent ad hoc sanctions.
20. Not routing of sales proceeds through consortium I member bank/ lenders to the company.
21. LCs issued for local trade I related party transactions without underlying trade transaction
22. High value RTGS payment to unrelated parties.
23. Heavy cash withdrawal in loan accounts.
24. Non production of original bills for verification upon request.
25. Significant movements in inventory, disproportionately differing vis-a-vis change in the turnover.
26. Significant movements in receivables, disproportionately differing vis-à-vis change in the turnover and/or increase in ageing of the receivables
27. Disproportionate change in other current assets
28. Significant increase in working capital borrowing as percentage of turnover
29. Increase in Fixed Assets, without corresponding increase in long term sources (when project is implemented).
30. Increase in borrowings, despite huge cash and cash equivalents in the borrower’s balance sheet
31. Frequent change in accounting period and/or accounting policies
32. Costing of the project which is in wide variance with standard cost of installation of the project
33. Claims not acknowledged as debt high
34. Substantial increase in unbilled revenue year after year.
35. Large number of transactions with inter-connected companies and large outstanding from such companies
36. Substantial related party transactions
37. Material discrepancies in the annual report
38. Significant inconsistencies within the annual report (between various sections)
39. Poor disclosure of materially adverse information and no qualification by the statutory auditors
40. Raid by Income tax /sales tax/ central excise duty officials
41. Significant reduction in the stake of promoter /director or increase in the encumbered shares of promoter/director.
42. Resignation of the key personnel and frequent changes in the management

Interview Based

A semi-structured interview was conducted by the authors with various officials of the banking industry and investigating agencies. Detailed projects can be made available on request. Thus, from the study, the authors were able to come up with the following insights and key findings:-

1. Fraud detection procedure in public sector banks: The authors analyzed the process of fraud detection and reporting in a public sector bank and who are the various players involved in this process. Following is a step by step illustration of the same (Figure 5). a) First, a fraud is internally reported to senior management of a bank. These may include chief general managers, executive directors, chairman and managing director. They may also be reported to vigilance department of the bank. b) If reported to the vigilance department of the bank, it investigates the fraud and then reports it to both senior management as well as the central vigilance commission (CVC) to whom they are required to report monthly. c) Although CVC can report fraud directly to investigating agencies like CBI, usually final decision to either report fraud to an external agency or to deal with it internally is made by senior management of the bank. Depending upon size of the bank, amount of money involved in fraudulent activity and number of third parties involved, senior management may choose to deal with the fraud internally or file an FIR and report it to either local police or CBI. d) A committee of the RBI also independently monitors fraudulent behaviour in banks and reports its observations on quarterly basis to central board of the RBI. The board may then report the matter to either central vigilance commission or ministry of finance (MoF). e) Auditors, during the course of their audit, may come across instances where transactions in accounts or documents point to possibility of fraudulent transactions in accounts. In such a situation, auditor may immediately bring it to the notice of top management and if necessary to audit committee of board (ACB) for appropriate action. f) Employees can also report...
fraudulent activity in an account, along with the reasons in support of their views, to the appropriately constituted authority (Table 1), under the whistle blower policy of the bank, who may institute a scrutiny through the fraud monitoring group (FMG). The FMG may ‘hear’ the concerned employee in order to obtain necessary clarifications. Protection should be available to such employees under the whistle blower policy of the bank so that fear of victimization does not act as a deterrent.

Poor appraisal system and monitoring mechanism in PSBs: The initial project appraisal process in PSBs is as good as that of PVBs. But monitoring post sanction of loan is weaker in PSBs compared to the PVBs on account of diverse loan portfolio, lack of expertise and modern technological resources, and lack of manpower and motivated employees, who are not appropriately incentivized to detect early frauds or prevent them. 5. Corporate governance and other HR issues: The root cause of weak corporate governance at highest level is directly linked to the very process of appointment of highest level of officials and poor compensation structure of highest level functionaries. The weakness in selection process for top level management as documented in RBI (2014b) results into weak governance at the highest level. Also, there is a serious issue in terms of pay structure in higher echelons of PSBs, which is markedly lower than their counterparts in PVBs. The only good factor in PSBs is prestige of a post that a person holds. Frauds also result from lack of awareness of staff towards appropriate procedures in place and red flags they should be aware of. Technology related frauds are primarily due to non-adherence to standard procedures and systems in place, by the employees. Even when any employee detects some fraudulent activities in existence involving people in power, whistle blower protection policy does not guarantee adequate safety.