Frauds in the Indian Banking

Vikas S Upadhyay
Research Scholar
Department of Mechanical Engineering
Shri GPM College, Mumbai, Maharashtra, India

Abstract— In this paper, we have attempted to identify the issues and problems associated with banking frauds. Fraud is a concept that is generally understood, but whose characteristics are often not recognized until it is too late. The potential damage, financial and reputational, means that this risk cannot be ignored. Combating fraud requires an understanding of how and why it occurs and the way by which it can be minimized. As the pressure on management to maintain income and earnings increases, the incentive to commit fraud is higher. The above issues are the main subject of the paper. Its most interesting part refers to real fraud cases that have occurred in the banking system. These cases reveal the causes leading to fraud. Finally, the paper asks how the risk of fraud can be prevented.

Key words: Fraud, Scam, Prevention, Suggestion and Conclusion

I. INTRODUCTION

Fraud is a global problem. Fraud can occur in any organization at any time, fraud is dynamic. Significant frauds are now increasing as the global financial crisis has taken hold. Most fraudulent acts are perpetrated by employees who understand the internal operations at their workplace and take advantage of internal control weaknesses. But what does fraud really mean?

Fraud can be considered any falsification or misrepresentation by customer, employee or any third party with the intention to gain undeserved benefit. Generally speaking, an act is considered fraud when losses occur, whilst the gain from this act is not simply about money. Any type of advantage is a gain. What do people often steals or gain? It can be cash, equipment, and intellectual property, information for personal gain, name or reputation.

Fraud performed through the presentation of false information, involving or obtaining a loan unrightfully by, for example, registering fictitiously mortgage properties that do not exist, claiming inflated prices for properties, or using a property that belongs to someone else. The loan application is made with the intent not to repay the loan

II. THE OBJECTIVE OF THIS STUDY WAS THREE FOLD.

1) To study Indian banking and financial system along with current processes and regulations in place
2) To identify issues in the current system and reasons for these issues
3) To suggest recommendations that can help the system tackle these issues

III. TYPES OF BANKING FRAUDS

1) Stolen check -: Fraudsters may seek access to facilities such as mailrooms, post offices, offices of a tax authority, a corporate payroll or a social or veterans' benefit office, which process cheques in large numbers. The fraudsters then may open bank accounts under assumed names and deposit the cheques, which they may first alter in order to appear legitimate, so that they can subsequently withdraw unauthorized funds.
2) Alternatively, forgers gain unauthorized access to blank cheque books, and forge seemingly legitimate signatures on the cheques, also in order to illegally gain access to unauthorized funds.
3) Cheque kiting -: Cheque kiting exploits a banking system known as "the float" wherein money is temporarily counted twice. When a cheque is deposited to an account at Bank X, the money is made available immediately in that account even though the corresponding amount of money is not immediately removed from the account at Bank Y at which the cheque is drawn. Thus both banks temporarily count the cheque amount as an asset until the cheque formally clears at Bank Y. The float serves a legitimate purpose in banking, but intentionally exploiting the float when funds at Bank Y are insufficient to cover the amount withdrawn from Bank X is a form of fraud.
4) Forgery and altered cheques -: Fraudsters have altered cheques to change the name (in order to deposit cheques intended for payment to someone else) or the amount on the face of cheques, simple altering can change $100.00 into $100,000.00, although transactions of this value are subject to investigation as a precaution to prevent fraud as policy.
5) Instead of tampering with a real cheque, fraudsters may alternatively attempt to forge a depositor's signature on a blank cheque or even print their own cheques drawn on accounts owned by others, non-existent accounts, etc. They would subsequently cash the fraudulent cheque through another bank and withdraw the money before the banks realize that the cheque was a fraud.
6) Accounting fraud -: In order to hide serious financial problems, some businesses have been known to use fraudulent bookkeeping to overstate sales and income, inflate the worth of the company's assets, or state a profit when the company is operating at a loss. These tampered records are then used to seek investment in the company's bond or security issues or to make fraudulent loan applications in a final attempt to obtain more money to delay the inevitable collapse of an unprofitable or mismanaged firm. Examples of accounting frauds: Enron and WorldCom and Ocala Funding. These companies "cooked the books" in order to appear as though they had profits each quarter, when in fact they were deeply in debt.
7) Demand draft fraud -: Demand draft (DD) fraud typically involves one or more corrupt bank employees. Firstly, such employees remove a few DD leaves or DD books from stock and write them like a regular DD. Since they are insiders, they know the coding and

All rights reserved by www.ijsrd.com

punching of a demand draft. Such fraudulent demand drafts are usually drawn payable at a distant city without debiting an account. The draft is cashed at the payable branch. The fraud is discovered only when the bank's head office does the branch-wise reconciliation, which normally take six months, by which time the money is gone.

8) Remotely created check fraud -: Remotely created checks are orders of payment created by the payee and authorized by the customer remotely, using a telephone or the internet by providing the required information including the MICR code from a valid check. They do not bear the signatures of the customers like ordinary cheques. Instead, they bear a legend statement "Authorized by Drawer". This type of instrument is usually used by credit card companies, utility companies, or telemarketers. The lack of signature makes them susceptible to fraud. The fraud is considered DD fraud in the US.
9) Fraudulent loans -: One way to remove money from a bank is to take out a loan, a practice bankers would be more than willing to encourage if they knew that the money will be repaid in full with interest. A fraudulent loan, however, is one in which the borrower is a business entity controlled by a dishonest bank officer or an accomplice; the "borrower" then declares bankruptcy or vanishes and the money is gone. The borrower may even be a non-existent entity and the loan merely an artifice to conceal a theft of a large sum of money from the bank. This can also seen as a component within mortgage fraud (Bell, 2010)
10) Wire transfer fraud -: Wire transfer networks such as the international SWIFT interbank fund transfer system are tempting as targets as a transfer, once made, is difficult or impossible to reverse. As these networks are used by banks to settle accounts with each other, rapid or overnight wire transfer of large amounts of money are commonplace; while banks have put checks and balances in place, there is the risk that insiders may attempt to use fraudulent or forged documents which claim to request a bank depositor's money be wired to another bank, often an offshore account in some distant foreign country.
11) There is a very high risk of fraud when dealing with unknown or uninsured institutions.
12) Bill discounting fraud -: Essentially a confidence trick, a fraudster uses a company at their disposal to gain confidence with a bank, by appearing as a genuine, profitable customer. To give the illusion of being a desired customer, the company regularly and repeatedly uses the bank to get payment from one or more of its customers. These payments are always made, as the customers in question are part of the fraud, actively paying any and all bills raised by the bank. After time, after the bank is happy with the company, the company requests that the bank settles its balance with the company before billing the customer. Again, business continues as normal for the fraudulent company, its fraudulent customers, and the unwitting bank. Only when the outstanding balance between the bank and the company is sufficiently large, the company takes the payment from the bank, and the company and its customers disappear, leaving no-one to pay the bills issued by the bank.
13) Payment card fraud -: Credit card fraud is widespread as a means of stealing from banks, merchants and clients.
14) Booster cheques -: A booster cheque is a fraudulent or bad cheque used to make a payment to a credit card account in order to "bust out" or raise the amount of available credit on otherwise-legitimate credit cards. The amount of the cheque is credited to the card account by the bank as soon as the payment is made, even though the cheque has not yet cleared. Before the bad cheque is discovered, the perpetrator goes on a spending spree or obtains cash advances until the newly-"raised" available limit on the card is reached. The original cheque then bounces, but by then it is already too late.

IV. HERE ARE SOME OF THE BIGGEST SCAMS THAT SHOOK THE COUNTRY'S BANKING SYSTEM AND RAISED SEVERAL QUESTIONS

A. 2011

In 2011, investigative agency CBI revealed that executives of certain banks such as the Bank of Maharashtra, Oriental Bank of Commerce and IDBI created almost created 10,000 fictitious accounts, and an amount of Rs 1.5 billion or Rs 1,500 crore worth loans was transferred.

B. 2014

Three years later in 2014, Mumbai Police filed nine FIRs against a number of public sector related to a fixed deposit fraud to the tune of Rs 7 billion or Rs 700 crore. In the same year, Electrotherm India, which defaulted payment of Rs 4.36 billion or Rs 436 crore to the Central Bank. Apart from that, Bipin Vohra, a Kolkata-based industrialist allegedly defrauded the Central Bank of India by receiving a loan of Rs 14 billion using forged documents.

- Besides, another scam that was unfolded in 2014 was the bribe-for-loan scam involving ex-chairman and MD of Syndicate Bank SK Jain for involvement in sanctioning Rs 80 billion or Rs 8,000 crore.
- In 2014, Vijay Mallya was also declared a willful defaulter by Union Bank of India, following which other banks such as SBI and PNB followed suit.

C. 2015

In 2015, another fraud that raised eyebrows involved employees of Jain Infraprojects, who defrauded Central Bank of India to the tune of over Rs two billion. In the same year, employees of various banks were involved in a foreign exchange scam involving a phony Hong Kong corporation. They had defrauded the systems to move out Rs 60 billion.

D. 2016

One of the biggest banking frauds of 2016 is the one involving Syndicate Bank, where almost 380 accounts were opened by four people, who defrauded the bank of Rs 10 billion using fake cheques, LoUs and LIC policies.

All rights reserved by *www.ijsrd.com*

E. 2017

- In 2017, Mallya's debt - owing to defunct Kingfisher Airlines - rises to Rs 9.5 billion or Rs 9,500 crore to IDBI and other bank branches. CBI prepares chargesheet but he had fled the country in 2016. Currently residing in the UK, Mallya's extradition is being sought at the country's Westminster Court.
- In the same year, Winsome Diamonds - also known to be India's second largest corporate defaulter - came under the scanner after CBI booked six cases against the group and the companies under it. This case is similar to the one observed in the fresh bank fraud involving Nirav Modi group: Letters of Undertaking were issued by Indian Banks to Jatin Mehta's Winsome Diamonds. It may be noted that the gaps were first discovered in 2014. From mid-2013 the group failed to payback its debts, and was declared a willful defaulter by banks. The total debt amounts to almost Rs 7,000 crore.
- Another case that grabbed eyeballs in the same years involved Deccan Chronicle Holdings for causing a loss of Rs 11.61 billion; CBI registered FIR against five PSBs and six chargesheets were filed against the company.
- A Kolkata business tycoon Nilesh Parekh, a promoter of Shree Ganesh Jewellery House, was arrested by CBI in 2017 for causing a loss of Rs 22.23 billion to at least 20 banks. Parekh, arrested at Mumbai airport last year, allegedly defrauded banks by diverting loan money via shell companies in Hong Kong, Singapore, and the UAE.
- In this case, CBI filed a case against the former zonal head of the Bank of Maharashtra and a director of a private logistics company based in Surat, owing to an alleged scam involving Rs 8.36 billion.

F. 2018

Last but not the least by any means, the fresh bank fraud to the tune of Rs 11,450 crore involving diamond merchant Nirav Modi. It has come to light that the company, in connivance with retired employees of PNB, got at least 150 Letter of Undertakings (LoUs), allowing Nirav Modi Group to defraud the bank and many other banks who gave loans to him. An Indian Express report says that in addition to the Rs 11,450 crore, Modi also defrauded 17 other banks of Rs 3,000 crore. In this case, however, fake LoUs were recycled by the diamond jewellery group and illegally issued to other banks for borrowing money. Nirav Modi, his family and partners have fled the country and an exclusive report by TIMES NOW reveals that he is currently in the United States.

- Another case that came to light this year concerns a former Andhra Bank director, who was arrested by Enforcement Directorate, in connection to an alleged Rs 5 billion bank fraud case, involving a Gujarat-based pharma firm.

V. BANK ACCOUNT FRAUD PREVENTION

The banking industry has developed the following fraud prevention tools:

- Positive pay is a type of account reconciliation service provided by banks. In positive pay, a bank compares checks that it receives for payment against the record of the checks issued by the government. If the bank receives a check that does not match the information (date, check number, and amount) in the government's record, it identifies it as an exception item (i.e., a non-conforming positive pay item). Payee positive pay is an enhanced positive pay service that requires the validation of the payee name in addition to validating the date, check number, and amount.
- ACH blocks and filters stop any attempt by an outside entity to process an ACH transfer and remove funds from a checking account without prior permission. ACH blocks prevent all disbursements from an account. ACH filters prevent disbursements that do not match a list of pre-authorized transactions or identification numbers. ACH filters involve: (a) giving prior permission to certain approved business partners to draw upon the account, (b) establishing an approval process for pending ACH transmissions, and/or (c) setting maximum dollar limits on ACH debit transactions.
- Reconciliation tools allow governments to extract information from their bank or have information sent from their bank that assists the government in performing period end reconciliation of bank accounts. The bank may also provide a tool that completes a full reconciliation of the account and produces detailed reports of reconciled items.
- Intra-day access allows a government to see bank account transactions that occur at various times throughout the business day. The information may be accessed via online systems provided by the bank, as well as through other methods including fax, email, and direct transmission of data from the bank to the government's computer systems.
- Universal Payment Identification Codes (UPIC) may be used instead of the government's bank account numbers so that the government's account numbers are not disclosed.

A. Recommendation:

GFOA recommends that governments consider the following steps to protect themselves against bank account fraud:

B. Internal Controls

- Conduct periodic surprise audits and annual reviews of procedures.
- Provide for the physical security of all checks.
  - Maintain check images in preference to paper copies.
  - Keep check stock in a locked and secure location with a formal inventory listing maintained. Secure check stock daily. Remove continuous check stock from printers. Lock and secure check specific printers. Consider the use of blank or unprinted check stock with inventory control numbers. The

All rights reserved by *www.ijsrd.com*

actual check number may be generated through the financial accounting system.
  - Physically void returned checks and check copies, and retain in a locked and secure location or destroy on a schedule.
  - Provide for the temporary physical security of electronically deposited checks, including storage in a secure facility, timely destruction such as secure shredding. (The depositing government is liable for any fraudulent usage of these checks.)
- Ensure appropriate security over signature plates, cards, and software.
- Require additional review process for all checks over a specified amount.
- Consider using a Controlled Disbursement account, to the extent permitted by law, for all payroll and Accounts Payable disbursements to provide additional control. It is preferable to make payments via batch ACH (direct deposit) for both Payroll and Accounts Payable as opposed to checks to reduce fraud potential and payment expenses.
- Require two party authorizations (initiation and release) on all wires and ACH files.
- Require daily staff reconciliation of wires and ACH releases.
- Ensure proper segregation of duties among staff initiating, authorizing, preparing, signing, and mailing payments and reconciling bank statements.
- Review signature cards and authority levels whenever any changes occur and annually at a minimum. Remove individuals from bank transaction authority immediately upon resignation or termination.
- Review all bank accounts at least annually. Consolidate or eliminate bank accounts that are not frequently utilized.
- Depending on the complexity, size and volume, consider segregating cash inflow and outflow in separate accounts to allow for placement of appropriate fraud prevention practices and products. When appropriate (i.e. if no restrictions exist) these types of separate accounts should be maintained as Zero Balance Accounts (ZBAs) that are swept into the governmental entity's concentration account.
- Ensure that controls exist for the storage and destruction of all documents that contain account and other related information.
- Determine that appropriate controls are present if employees access the governments financial and banking systems from remote sites (i.e., restrict the sharing of files).
- On at least an annual basis, request the government's legal counsel to research changes in laws that shift liability for fraudulent transactions to the government.

C. Fraud Prevention Measures in Cooperation with Government's Financial Institution(s)

- Implement positive pay, or preferably payee positive pay, on all disbursement bank accounts and reconcile exceptions daily. Positive pay is the single best fraud prevention tool available. If a government's bank offers a positive pay service and the government chooses not to utilize it, then the government (not the bank) will be liable for fraudulent transactions.
  - Instruct the bank to return all non-conforming positive pay items as the default instruction.
  - Ensure that a clear policy exists to separate responsibilities between staff approving positive pay exceptions and staff initially requesting and/or preparing the check.
  - Avoid reverse positive pay because with this service the liability remains with the government.
- Direct the bank to reject or block any and all withdrawals not initiated by the government from accounts that only accept deposits.
- Place ACH filters and/or blocks on all accounts.
  - Place total or selective ACH blocks on all disbursement accounts. Selective ACH blocks, also known as ACH filters, allow electronic debits to occur only for pre-designated transactions.
  - Develop a formal plan to review ACH blocks/filters. This should be done on an annual basis, at a minimum.
- Consider the use of Universal Payments Identification Codes (UPIC) for all receivables accounts.
- Ensure that your financial institutions provides for multi-factor identification for on-line banking services involving transactions and administrative functions. Ensure separation of duties (initiation and release/approved) for financial transactions and administration of the on-line system. Multi-factor identification may include numerous passwords and/or utilization of user specific tokens.
- Ensure that your financial institution provides a quarterly listing, by account, of all approved signers and access-only individuals.
- Utilize bank reconciliation services to reduce time on reconciliation and focus on exception items.
- Discuss enhanced or new account security features with your financial institution on at least an annual basis.

VI. SUGGESTION

A. Multi-Factor Authentication

The best approach is to start with a multi-factor authentication/multi-layered security structure. This is what Romeo is seeing from the institutions that are successfully thwarting fraud. "Remember, there is no one silver bullet that will solve this problem, so if you put all your hope in a single solution, you'll get compromised, and the intruder will have everything."

This multi-layered approach from a software perspective, combined with old-fashioned out-of-band phone calls to the customer to confirm a questionable transaction, can cut the institution's headaches and the business' fraud losses.

In the old days, Romeo says, calendars were put in place for all set transactions for all accounts, whether they were large corporate or small businesses. "If they had a weekly payroll, that only went out once a week, and then all

All rights reserved by *www.ijsrd.com*

of a sudden we saw something going out every day -- that would be a red flag; we would question it," he says.

B. Banks: Monitor Transactions

In his days in bank operations, Romeo says, the bank used to set up daily limits on each user. "We used to set these limits on our mainframe processor in the bank, along with file limits and batch limits, so if there were something added, or out of the ordinary, we would spot it." Another thing to watch for is a whole lot of activity right under $9,000. "Because the fraudsters know they won't draw suspicion of a bank if they fly under $10,000 mark."

C. Businesses: Reconcile Corporate Accounts daily

For businesses, Romeo recommends reconcilement of banking accounts and transactions on a daily basis -- either at end of day or at least at the beginning. "This will help catch any transactions you didn't make, and the sooner you bring it to your bank's attention, the better chance to retrieve the money, with the bank doing a recall or reversal of the transaction. The longer you wait, the less likely it is that you'll see that money recovered."

D. Employ Dual, Triple Controls

Dual controls at the corporate side are, at the very least, table stakes. Romeo suggests even triple controls, where one person creates the transaction, a second person approves it, and then a third person actually sends the transaction."If you don't have the people, then set up the ACH transactions with the institution, an out of band confirmation, whether it is a phone call to confirm that you've sent it, and confirmation of the correct information was received," he notes. This can be done live or through an automated voice response system. Usually, only one person would have the password and ID to call the bank, which would be totally separate from the person's computer.

E. Raise Fraud Awareness

Finally, Romeo says, continuous education of business customers is important. At the national level, this problem of corporate account takeover has gotten real attention. But real solutions won't come until financial institutions and their corporate accounts alike realize the real risks they face - and simple solutions they can implement to help mitigate those risks.

VII. CONCLUSIONS

The frauds may be primarily due to lack of oversight of top management, faulty incentive mechanism in place for employees, collusion between the staffs or corporate borrowers and third party agencies, weak regulatory system, lack of appropriate tools and technologies in place to detect the early warning signals of a fraud, lack of awareness of bank employees and customers, lack of coordination among different banks across India and abroad. Towards filling the gaps, major recommendations included improvement in culture and attitude of top management of the firm, giving priority to awareness enhancement among employees, adequate information disclosure to appropriate authorities, financial awareness enhancement of investigative agencies, strengthening and enhancing the scope of internal supervisory bodies, strengthening regulatory system for third party authorities' regulation, establishment of central repository system for fraud related information sharing across different banks, IT empowerment. Going forward, the implementation of recommendations in the above-mentioned dimensions should help in strengthening the banking sector in India and go a long way in handling the frauds proactively.

REFERENCES

[1] *Evaluating Internal Controls: A Local Government Manager's Guide*, Stephen J. Gauthier, GFOA, 1996.
[2] *Banking Services: A Guide for Governments*, Nick Greifer, GFOA, 2004.
[3] Uniform Commercial Code as cited on the following Website: http://www.law.cornell.edu/ucc/ucc.table.htm
[4] Papanek J., Frydrych O. and Wolf T. (2009), 'Fraud Risk Management RI Workshop', page 11.
[5] Uline, B. J. (2007), 'Fraud Awareness and Prevention. The Detection of Fraud Begins with You', Fraud Examiner's Manual, ACFE.
[6] Wikipedia
[7] Times Now
[8] Sharma, Manoj. "Framework for dealing with loan frauds" (2015), RBI Circular, DBS.CO.CFMC.BC.No.007, 7 May 2015
[9] KPMG, "India Fraud Survey 2012." KPMG. Web, 2012.
[10] Arora, P.K. "Monitoring of large value frauds by the Board of Directors." Reserve Bank of India Circular, DCBR.BPD PCB Cir. No. 10, 7 January, 2015.

All rights reserved by *www.ijsrd.com*