Chapter 6 – Cyber Fraud

Introduction:

With the advances in information technology, most banks in India have migrated to core banking platforms and have moved transactions to payment cards (debit and credit cards) and to electronic channels like ATMs, Internet Banking and Mobile Banking. Fraudsters have also followed customers into this space. However, the response of most of the banks to frauds in these areas needs further improvement, thereby avoiding putting the entire onus on the customer. There is also a lack of clarity amongst banks on the reporting of these instances as frauds.

A need is therefore felt to have an industry wide framework on fraud governance with particular emphasis on tackling electronic channel based frauds. This note endeavours to bring out the challenges and suggests a framework which can be implemented across banks to effectively tackle the electronic fraud menace. It would be useful to recall the definition of fraud at this stage.

> *'A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank'.*

This definition has been recommended as per para 9.1 of the Report of the Study Group on Large Value Bank Frauds set up by the Reserve Bank of India in 1997. It follows that like other bank frauds, various IT related frauds need to get captured through the fraud reporting system and banks should take adequate steps to mitigate such risks.

1. Roles/Responsibilities and Organizational structure for fraud risk management:

(a) Indian banks follow the RBI guideline of reporting all frauds above Rs.1 crore to their respective Audit Committee of the Board. Apart from this, banks are also putting up a detailed annual review of frauds to their Audit Committee of the Board. The Board for Financial Supervision (BFS) of RBI has observed that in terms of higher governance standards, the fraud risk management and fraud investigation must be 'owned' by the bank's CEO, Audit Committee of the Board and the Special Committee of the Board.

(b) Special Committee of the Board for monitoring large value frauds

Banks are required to constitute a special committee for monitoring and follow up of cases of frauds involving amounts of ₹1 crore and above exclusively, while the Audit Committee of the Board (ACB) may continue to monitor all the cases of frauds in general. The major function of the special committee is to monitor and review all the frauds of Rs.1 crore and above so as to:

- Identify the systemic lacunae if any that facilitated perpetration of the fraud and put in place measures to plug the same
- Identify the reasons for delay in detection, if any, reporting to top management of the Bank and RBI
- Monitor progress of CBI/Police investigation and recovery position
- Ensure that staff accountability is examined at all levels in all the cases of frauds and staff side action, if required, is completed quickly without loss of time

- Review the efficacy of the remedial action taken to prevent recurrence of frauds, such as strengthening of internal controls
- Put in place other measures as may be considered relevant to strengthen preventive measures against frauds.

The Special Committee should meet and review as and when a fraud involving an amount of ₹1 crore and above comes to light. Further, it is desirable that a meeting of the Special Committee should be convened once a quarter, to deliberate on the progress of the prevention initiatives, staff accountability and progress of investigation by the police authorities and recoveries if any, in such cases. Most retail cyber frauds and electronic banking frauds would be of values less than ₹1 crore and hence may not attract the necessary attention of the Special Committee of the Board. Since these frauds are large in number and have the potential to reach large proportions, it is recommended that the Special Committee of the Board be briefed separately on this to keep them aware of the proportions of the fraud and the steps taken by the bank to mitigate them. The Special Committee should specifically monitor the progress of the mitigating steps taken by the bank in case of electronic frauds and the efficacy of the same in containing fraud numbers and values.

(c) Separate Department to manage frauds

The activities of fraud prevention, monitoring, investigation, reporting and awareness creation should be owned and carried out by an independent group in the bank. The group should be adequately staffed and headed by a senior official of the Bank, not below the rank of General Manager.

(d) Fraud review councils

Fraud review councils should be set up by the above fraud risk management group with various business groups in the bank. The council should comprise of head of the business, head of the fraud risk management department, the head of operations supporting that particular business function and the head of information technology supporting that business function. The councils should meet every quarter to review fraud trends and preventive steps taken that are specific to that business group.

2. <u>Components of fraud risk management:</u>

(i) Fraud prevention practices

A strong internal control framework is the strongest deterrence for frauds. The fraud risk management department along with the business/operations/support groups, continuously reviews various systems and controls, to remove gaps if any, and to strengthen the internal control framework. The following are some of the fraud prevention practices that are recommended for banks.

(a) Fraud vulnerability assessments

Fraud vulnerability assessments should be undertaken across the bank by the fraud risk management group. Apart from the business and the operations groups, such assessment also cover channels of the bank such as branches, internet, ATM and phone banking, as well as international branches, if any. During the course of a vulnerability assessment, all the processes should be assessed based on their fraud risk. Controls need to be checked and improvements suggested for tightening the same. These should be reviewed in the fraud review councils.

'Mystery Shopping' is an important constituent of vulnerability assessment. Transactions are introduced in 'live' scenarios to test the efficacy of controls. The results of the mystery shopping exercises should be shared with the relevant groups in the fraud review councils and be used for further strengthening of controls.

(b) Review of new products and processes

No new product or process should be introduced or modified in a bank without the approval of control groups like compliance, audit and fraud risk management groups. The product or process needs to be analysed for fraud vulnerabilities and fraud loss limits to be mandated wherever vulnerabilities are noticed.

(c) Fraud loss limits

All residual/open risks in products and processes need to be covered by setting 'fraud-loss' limits. 'Fraud-loss' limits need to be monitored regularly by the fraud risk management group and a review needs to be undertaken with the respective business group when fraud loss amount reaches 90% of the limit set. In case it is difficult to set a fraud- loss limit, a limit on the total number or total value of frauds may be defined. For the purpose of deciding how much a product or a process has used up the limit set, the cumulative value of frauds in that product or process during the financial year needs to be considered.

(d) Root cause analysis

All actual fraud cases above ₹10 lakhs and cases where a unique modus operandi is involved, should be reviewed immediately after such a fraud is detected. The findings should be used to redesign products and processes and remove the gaps so that they do not recur.

(e) Data/information/system security

Most banks have incorporated several security measures for their documents, information, systems and customer deliverables such as cheque books/debit cards. Security measures have also been incorporated during delivery of instruments such as cards/cheque books/internet passwords to customers through couriers. Internet banking systems have security features such as separate transaction passwords, two factor authentication, multi-channel process for registering payees, upper limit on transaction value and SMS alerts to customers. It is also necessary that customer confidential information and other data/information available with banks is secured adequately to ensure that fraudsters do not access it to perpetrate fraudulent transactions. Appropriate steps need to be taken to ensure data/information/system security at the Bank, as indicated earlier in the report. Information security and appropriate access control procedures ensure that only employees who are required to know particular information have access to the same and can put through transactions. Further, a bank's systems need to be adequately secured to ensure that no un-authorised person carries out any system modifications/changes. Appropriate verification procedures should also be incorporated at all channels such as phone banking, ATMs, branches and internet to ensure that only genuine transactions are put through. All the above security measures should be under continuous review for further strengthening. Details in this regard were covered in chapter on information security.

(f) Know Your Customer (KYC) and know your employee/vendor procedures

A strong KYC process is the backbone of any fraud prevention activity. Such a process enables banks to prevent unscrupulous elements from gaining entry into the bank's environment, which gives them an opportunity to carry out their fraudulent intentions. Similarly, appropriate due diligence procedures before recruitment of employees and vendors is essential to prevent known fraudsters or people with fraudulent motives to

have access to a bank's channels. Banks have to implement strong procedures to carry out due diligence of potential customers, employees and vendors before they are enrolled.

Common KYC documents for account opening: The possibility of setting up an agency with which the customer can register for KYC certification may be examined. Once a customer registers with such an agency, banks can open accounts for customers without any documentation except the certification. The certificate can be checked by the bank online by referring to the website of the certification agency.

(g) Physical security

All banks have a dedicated team to take care of the security of the physical infrastructure. This team should conduct regular security audits of various offices to check for deviations/lapses. It is the responsibility of this team to ensure that physical assets and data copied on magnetic/optical media do not go out of the offices of the bank without authorisation.

(h) Creation of fraud awareness amongst staff and customers

Awareness on how to prevent and detect frauds is the basis of fraud management. Banks need to adopt various measures to create awareness amongst staff and customers. Some of the recommended measures are detailed in subsequent paragraphs in the document.

(ii) Fraud detection

a) Detection of fraud

Despite strong prevention controls aimed at fraud deterrence, fraudsters do manage to perpetrate frauds. In such cases, the earlier the fraud is detected, the better the chance of recovery of the losses and bringing the culprits to book. System triggers that throw up exceptional transactions, opening up channels that take note of customer/employee alerts/disputes, seeding/mystery shopping exercises and encouraging employees/customers/ well- wishers to report suspicious transactions/behaviours are some of the techniques that are used for detection of frauds. The exceptional/suspicious transactions/activities reported through these mechanisms should be investigated in detail.

b) Transaction monitoring

Banks should set up a transaction monitoring unit within the fraud risk management group. The transaction monitoring team should be responsible for monitoring various types of transactions, especially monitoring of potential fraud areas, by means of which, early alarms can be triggered. This unit needs to have the expertise to analyse transactions to detect fraud trends. This unit should work in conjunction with the data warehousing and analytics team within banks for data extraction, filtering, and sanitisation for transaction analysis for determining fraud trends. Banks should put in place automated systems for detection of frauds based on advanced statistical algorithms and fraud detection techniques.

c) Alert generation and redressal mechanisms

Appropriate mechanisms need to be established in banks, to take note of the disputes/exceptions or suspicions highlighted by various stakeholders including transaction monitoring teams in banks and to investigate them thoroughly. Banks should have a well publicised whistle blowing mechanism.

d) Dedicated email ID for reporting suspected frauds

Banks can have dedicated email IDs for customers to report any fraudulent activity that they may notice. A dedicated team can be created to reply to customer queries and concerns through the above email IDs. Phone banking officers and branch staff should also be trained on response to customers' queries and concerns on frauds.

e) Dedicated phone number for reporting suspected frauds

Banks may contemplate the setting up of a fraud helpline for customers and employees to enable them to report suspected frauds and seek tips on fraud prevention. By doing this, banks can make available one more avenue for early reporting and detection of frauds.

f) Mystery shopping and reviews

Continuous supervision and control by managers/supervisors on activities is important to detect any abnormal activity. However, considering a bank's size and scope, this needs to be supplemented by mystery shopping to detect system flaws and also to identify unscrupulous employees/vendors. Immediate action needs to be taken on the findings of such reviews.

g) Importance of early detection of frauds

A bank's fraud management function is effective if it is able to minimise frauds and when fraud occurs, is able to detect the fraud so that the loss is minimised.

(iii)Fraud investigation

The examination of a suspected fraud or an exceptional transaction or a customer dispute/alert in a bank shall be undertaken by:

- Fraud risk management group
- Specific committee of employees constituted to examine the 'suspected fraud'
- Regulatory or investigative authorities
- External agencies, if any, as appointed by the bank

a) Fraud Investigation function

It is widely accepted that fraud investigation is a specialised function. Thus, the fraud risk management group should undergo continuous training to enhance its skills and competencies. The first step in an investigation process is gathering the entire transaction details, documents and complete details of the customer/employee or vendor. In order to investigate into suspected cases, the group would adopt various advanced techniques including computer forensics, forensic accounting and tools to analyse large volumes of data.

The investigation team may conduct oral interviews of customers or employees to understand the background and details of the case. In case an interview of the person accused of fraud is required to be undertaken, the investigation group should follow a prescribed procedure and record statements appropriately. The investigation activities need to be carried out discreetly and within a specified time line. The investigating team should take into account all the relationships of the involved parties with the bank while investigating and submitting an investigation report. The investigation report will help the respective business groups take a decision on all the relationships of the customer with the Bank. The investigation report should conclude whether a suspected case is a fraud

and thereafter the report would form the basis for further actions such as regulatory reporting.

In case of employee involvement in the fraud, the investigation report may be the basis of staff accountability and HR actions. It may be noted that, during the course of the investigations, banks should adopt only means permitted by law, regulations and code of conduct of the bank and any inconvenience to customers or general public should be avoided. It is also important to note that certain investigations are best carried out by law enforcement authorities and the bank should refer cases to such authorities at the appropriate time, to enable them to carry out their responsibilities efficiently.

In case of need, the investigating team should seek the support of other specialised groups within the bank, such as the audit group to carry out investigations efficiently.

At times, investigation of a fraud wherein money has come into the country to an account in a bank through another bank in the same country needs to be done. The intermediary bank does not investigate or report the case stating that it is merely an intermediary while the recipient bank states that it has no knowledge of the transaction and is merely a recipient of the funds sent by the intermediary bank. In this case, it is clarified that the bank whose customer has received the money should investigate and report the case.

b) Recovery of fraud losses

The concerned group in a bank, in which the fraud has occurred, should make all out efforts to recover the amount lost. They may use specialised groups like legal or collections for this purpose. The investigation team may also be able to recover some amounts during the course of their investigation. The Police may also recover some amount during their investigation. This would be deposited in Court pending final adjudication. The bank should liaise with the Police and keep track of such amounts.

(iv)Reporting of frauds

As per the guidelines on reporting of frauds as indicated in the RBI circular, dated July 1, 2010, fraud reports should be submitted in all cases of fraud of ₹1 lakh and above perpetrated through misrepresentation, breach of trust, manipulation of books of account, fraudulent encashment of instruments like cheques, drafts and bills of exchange, unauthorised handling of securities charged to the bank, misfeasance, embezzlement, misappropriation of funds, conversion of property, cheating, shortages, irregularities, etc. It is further recommended that this should also include frauds in the electronic channels and the variants of plastic cards used by a bank and its customers for concluding financial transactions.

a) Determination of the fraud amount for reporting

It has been noted that there is a lack of uniformity regarding the amount of fraud to be reported to the RBI. Some banks report the net loss as the fraud amount (i.e. fraud amount minus recovery), while others report the gross amount. Some do not report a fraud if the entire amount is recovered. In the case of credit card frauds, some banks follow the practice of reporting the frauds net of chargeback credit received while others report the amount of the original transactions. To overcome such inconsistency, a uniform rule of reporting amounts involved in frauds is being recommended. For transaction banking frauds like cheque forgery, remittance frauds, internet banking, credit cards, cash shortages etc., the fraud amount is the amount of the transaction(s) that is/have been done fraudulently. For borrowal frauds, the amount reported should be the principal outstanding plus the interest due till the date of detection of fraud. Any

recoveries done subsequent to the detection of fraud should be reported as recovery and not deducted from the fraud amount.

b) Frauds in merchant acquiring business

A special mention needs to be made here of frauds done by collusive merchants who use skimmed/stolen cards on the POS terminals given to them by banks and then abscond with the money before the chargeback is received on the transaction. It is imperative that the bank which has provided acquiring services to such merchant, reports the case to RBI.

c) Frauds in ATM acquiring business

Also, it has been observed that in a shared ATM network scenario, when the card of one bank is used to perpetrate a fraud through another bank's ATM, there is a lack of clarity on who should report such a fraud. It is the bank acquiring the transaction that should report the fraud. The acquiring bank should solicit the help of the issuing bank in recovery of the money. The facts of the case would decide as to which bank will bear the loss.

d) Filing of police complaints

As per para 6 of the above circular, banks have to file a police complaint for all frauds of ₹ 1 lakh and above and for staff involvement in fraud cases of the value exceeding ₹10,000. These limits being set a few years ago, there is a case for these being enhanced to ₹2 lakh and ₹20,000 respectively. In the case of online frauds, since the jurisdiction is not clear, there is ambiguity on where the police complaint should be filed. Cybercrime cells are not present in every part of the country. The matter of having a separate cell working on bank frauds in each state police department authorised to register complaints from banks and get the investigations done on the same needs to be taken up with the respective police departments. Also, banks should readily share data and documents requested by the police even in cases where the bank in question is not the victim of the fraud but has been a receiver of fraudulent monies into its accounts.

(v) Customer awareness on frauds

a) Creation of customer awareness on frauds

Customer awareness is one of the pillars of fraud prevention. It has been seen that alert customers have enabled prevention of several frauds and in case of frauds which could not be avoided, helped in bringing the culprit to book by raising timely alerts. Banks should thus aim at continuously educating its customers and solicit their participation in various preventive/detective measures. It is the duty of all the groups in banks to create fraud risk awareness amongst their respective customers. The fraud risk management group should share its understanding of frauds with each group, identify areas where customer awareness is lacking and if required, guide the groups on programmes to be run for creation of awareness amongst customers. The groups should ensure that in each of their interaction with customers there is at least one message to make the customer aware of fraud risk.

The following are some of the recommended measures to create awareness amongst customers:

- Publications in leading newspapers
- Detailed 'do's and don'ts' on the web site of the bank
- Messages along with statement of accounts, either physical or online
- Messages printed on bank's stationery such as envelopes, card covers, etc.

- SMS alerts
- Message on phone banking when the customer calls
- As inserts or on the jackets of cheque books
- Posters in branches and ATM centres
- Interstitials on television and radio

It should be ensured that the communication to the customer is simple and aimed at making them aware of fraud risks and seeking their involvement in taking proper precautions aimed at preventing frauds. Such communication should be reviewed periodically by the fraud risk management group to judge its effectiveness.

(vi) Employee awareness and training

(a) Creation of employee awareness

Employee awareness is crucial to fraud prevention. Training on fraud prevention practices should be provided by the fraud risk management group at various forums. Banks may use the following methods to create employee awareness:

- Class room training programmes at the time of induction or during risk related training sessions
- Publication of newsletters on frauds covering various aspects of frauds and containing important message on fraud prevention from senior functionaries of the Bank
- E-learning module on fraud prevention
- Online games based on fraud risks in specific products or processes
- E-tests on prevention practices and controls
- Detailed 'do's and don'ts' put up on the worksite of the employee
- Safety tips flashed at the time of logging into Core Banking System (CBS), screen savers, etc.
- Emails sent by the respective business heads
- Posters on various safety measures at the work place
- Messages/discussions during daily work huddles

(b) Rewarding employees on fraud prevention

A positive way of creating employee awareness is to reward employees who have gone beyond their call of duty, and prevented frauds. Awards may be given to employees who have done exemplary work in preventing frauds. Details of employees receiving such awards may be published in the fraud newsletters.

3. <u>Industry-Wide Recommendations</u>

(a) To enhance investigation skills of the staff in the fraud risk management group, a training institute for financial forensic investigation may be set up by banks under the aegis of IBA. Faculty and material may be made available by banks and other forensic experts. International best practices on training and certification can be adopted by the training institute.

(b) The experience of controlling/preventing frauds in banks should be shared between banks on a regular basis. The standing forum provided by the Indian Bank's Association (IBA) can be used to share best practices and further strengthen internal controls at the respective banks. Banks have started sharing negative/fraudulent list of accounts through CIBIL Detect. Banks should also start sharing the details of employees who have defrauded them so that they do not get hired by other banks/financial institutions.

(c) Interbank co-operation: While most banks today actively co-operate in freezing funds when information is received from another bank, when it comes to refund of the funds lying in the account, there is no standard practice for refund between banks. Some banks require an indemnity to be signed by the recipient bank while others insist on a court order. There should be a general agreement on process among all banks to refund monies lying in fraudulent beneficiary's account.

(d) In the case of online frauds, since the jurisdiction is not clear, there is ambiguity on where the police complaint should be filed and customers/banks have to shuttle between different police units on the point of jurisdiction. Cybercrime cells are not present in every part of the country. The matter of having a separate cell working on bank frauds in each state police department authorized to register complaints from banks and get the investigations done on the same needs to be taken up with the respective police departments.

(e) There needs to multi-lateral arrangements amongst banks to deal with on-line banking frauds. Presently, due to lack of such an arrangement amongst banks, a customer may be required to interact with different banks/ organizations when more than one bank is involved. IBA could explore and facilitate such a mechanism.

(f) Working with law enforcement authorities*:* At each state, a Financial Crime Review Committee needs to be set up on frauds along the lines of Security Committee that has been set up by the RBI to review security issues in banks with the law enforcement authorities. The Committee can oversee the creation of awareness by banks amongst law enforcement agencies on new fraud types, especially technology based frauds. Banks and the Police should regularly meet to discuss fraud trends and challenges. Banks may also, subject to budgetary constraints, make available cyber forensic equipments and expertise to the Police by sponsoring such facilities.

KEY RECOMMENDATIONS:

1. Most retail cyber frauds and electronic banking frauds would be of values less than ₹1 crore and hence may not attract the necessary attention of the Special Committee of the Board. Since these frauds are large in number and have the potential to reach large proportions, it is recommended that the Special Committee of the Board be briefed separately on this to keep them aware of the proportions of the fraud and the steps taken by the bank to mitigate them. The Special Committee should specifically monitor the progress of the mitigating steps taken by the bank in case of electronic frauds and the efficacy of the same in containing fraud numbers and values.

2. The activities of fraud prevention, monitoring, investigation, reporting and awareness creation should be owned and carried out by an independent group in the bank. The group should be adequately staffed and headed by a senior official of the Bank, not below the rank of General Manager/DGM.

3. Fraud review councils should be set up by the above fraud risk management group with various business groups in the bank. The council should comprise of head of the business, head of the fraud risk management department, the head of operations supporting that particular business function and the head of information technology supporting that business function. The councils should meet every quarter to review fraud trends and preventive steps taken that are specific to that business group.

4. Various fraud prevention practices need to be followed by banks. These include fraud vulnerability assessments, review of new products and processes, putting in place

fraud loss limits, root cause analysis for actual fraud cases above Rs.10 lakhs, reviewing cases where a unique modus operandi is involved, ensuring adequate data/information security measures, following KYC and Know your employee/vendor procedures, ensuring adequate physical security, sharing of best practices of fraud prevention and creation of fraud awareness amongst staff and customers.

5. Banks have started sharing negative/fraudulent lists of accounts through CIBIL Detect. Banks should also start sharing the details of employees who have defrauded them so that they do not get hired by other banks/financial institutions.

6. Quick fraud detection capability would enable a bank to reduce losses and can also serve as a deterrent to fraudsters. Various important requirements recommended in this regard include setting up a transaction monitoring group within the fraud risk management group, alert generation and redressal mechanisms, dedicated e-mail id and phone number for reporting suspected frauds, mystery shopping and reviews.

7. Banks should set up a transaction monitoring unit within the fraud risk management group. The transaction monitoring team should be responsible for monitoring various types of transactions, especially monitoring of potential fraud areas, by means of which, early alarms can be triggered. This unit needs to have the expertise to analyse transactions to detect fraud trends. This unit should work in conjunction with the data warehousing and analytics team within banks for data extraction, filtering, and sanitisation for transaction analysis for determining fraud trends. Banks should put in place automated systems for detection of frauds based on advanced statistical algorithms and fraud detection techniques.

8. It is widely accepted that fraud investigation is a specialised function. Thus, the fraud risk management group should undergo continuous training to enhance its skills and competencies.

9. Apart from the categories of fraud that need to be reported as per RBI circular dated July 2, 2010 , it is recommended that this should also include frauds in the electronic channels and the variants of plastic cards used by a bank and its customers for concluding financial transactions.

10. It has been noted that there is lack of uniformity regarding the amount of fraud to be reported to RBI. Some banks report the net loss as the fraud amount (i.e. fraud amount minus recovery), while others report the gross amount. Some do not report a fraud if the entire amount is recovered. In the case of credit card frauds, some banks follow the practice of reporting the frauds net of chargeback credit received while others report the amount of the original transactions. To overcome such inconsistency, a uniform rule of reporting amounts involved in frauds is being recommended.

11. A special mention needs to be made here of frauds done by collusive merchants who use skimmed/stolen cards on the POS terminals given to them by banks and then abscond with the money before the chargeback is received on the transaction. Many banks do not report such cases stating that the banks which have issued the cards are the ones impacted. However, in these cases, the merchants cause undue loss to the bank, by siphoning off the credit provided. Hence such cases should be reported as frauds.

12. Also, it has been observed that in a shared ATM network scenario, when the card of one bank is used to perpetrate a fraud through another banks' ATM, there is a lack of clarity on who should report such a fraud. It is the bank acquiring the transaction that

should report the fraud. The acquiring bank should solicit the help of the issuing bank in recovery of the money.

13. In the case of online frauds, since the jurisdiction is not clear, there is ambiguity on where the police complaint should be filed and customers/banks have to shuttle between different police units on the point of jurisdiction. Cybercrime cells are not present in every part of the country. The matter of having a separate cell working on bank frauds in each state police department authorised to register complaints from banks and get the investigations done on the same needs to be taken up with the respective police departments.

14. Customer awareness is one of the pillars of fraud prevention. It has been seen that alert customers have enabled prevention of several frauds and in case of frauds which could not be avoided, helped in bringing the culprit to book by raising timely alerts. Banks should thus aim at continuously educating its customers and solicit their participation in various preventive/detective measures. It is the duty of all the groups in banks to create fraud risk awareness amongst their respective customers.

15. Employee awareness is crucial to fraud prevention. Training on fraud prevention practices should be provided by the fraud risk management group at various forums.

16. A positive way of creating employee awareness is to reward employees who have gone beyond their call of duty, and prevented frauds. Awards may be given to employees, who have done exemplary work in preventing frauds. Details of employees receiving such awards may be published in the fraud newsletters.

17. To enhance investigation skills of the staff in the fraud risk management group, a training institute for financial forensic investigation may be set up by banks under the aegis of IBA.

18. The experience of controlling/preventing frauds in banks should be shared between banks on a regular basis. The standing forum provided by the Indian Bank's Association (IBA) can be used to share best practices and further strengthen internal controls at the respective banks.

19. There should be a general agreement on the process among all banks to refund monies lying in a fraudulent beneficiary's account.

20. There needs to multi-lateral arrangements amongst banks to deal with on-line banking frauds. Presently, it is noticed that there is lack of such an arrangement amongst banks and the customer is required to interact with different banks/ organizations when more than one bank is involved. IBA could facilitate such a mechanism.

21. At each state, a Financial Crime Review Committee needs to be set up on frauds along the lines of Security Committee that has been set up by the RBI to review security issues in banks with the law enforcement authorities. The Committee can oversee the creation of awareness by banks among law enforcement agencies on new fraud types, especially technology based frauds.