SUPREMO AMICUS

VOLUME 3 | JAN | 2018 ISSN: 2456-9704

ONLINE BANKING FRAUDS AND ROLE OF GOVERNMENT TO CURB IT: WITH SPECIAL REFERENCE TO INDIA

BY PARISHA SINGH
FROM GUJARAT NATIONAL LAW UNIVERSITY

ABSTRACT

The essay focuses on the distress caused by online fraud, in banking sector in India. In many countries introduction of cashless economy can be seen as steps in right direction, similarly demonetization of currency by the present government has promoted cashless transaction widely in India. Cyber crimes are increasing at par with transactions done online. The cyber space is increasingly used by organized criminal group to target credit card, bank account, and other transactional instrument for fraudulent transactions. This essayenvisages on the kinds of cyber frauds faced by banks and the reforms taken by the RBI and the government to deal with those fraudulent activities. the paper primarily focuses on is, whether the Indian banking sector even ready for such a reform in the economy? Are we technologically advanced enough to adopt to such a change?

INTRODUCTION

Cybercrime today is an all around organized multi-million-dollar business, executed by proficient programmers who approach better assets as far as man and machine than any organization. Most organizations are shocked as they are caught off guard for such an assault. A lot of our basic framework is associated with the internet. With government activities of Smart Cities and Digital India, all the foundation is associated with each other through IOT (Internet of things) and web, in this manner this risk is amplified and it requires more prominent concentration in execution of preventive, analyst and arranged/practiced reaction[1].

Objectives of the study is to analyze the increase in the fraud in bank in India and whether India is ready for such a reform in the country?The economic growth of any nation and its security, whether internal or external, and competiveness depends on how well is its cyberspace secured and protected. The increase use of digital means, for online banking has increased the risks of online frauds. The maximum offenders came from the age group of 18-30.This research attempts to analyze the concerns of cyber threats to the banking sector by

[1] Lalit Wadhwani, Crime and Security in The New Age: How Technology Has Disrupted National Security (Mar 18,2016) http://www.freepressjournal.in/business/crime-and-security-in-the-new-age-how-technology-has-disrupted-national-security/806233.

highlighting the underlying modus operandi. It focusses on the preparedness of the financial organizations to deal with incidents related to Cyber Crime.

In a recent study RBI has reported over 8,765cases were reported by banks in 2012-13 and figures for consequent three years are 9,500 (2013-14), 13,083 (2014-15) and 11,997 (in the first nine months of 2015-16) respectively.[2]These cases may be very small in number in number for a country as big as India with population of 1.2 billion, even though according to the reports India is third in rank after USA and Japan, which are most affected with online malware in 2014.There shall be no room left for such uncritical satisfaction in a country where the government actively envisages for every citizen to have account in bank and has indulged into developing schemes even for the rural sector welfare.However, another report entitled *Cyber and Network Security Framework*, revealed that the total number of cybercrimes in all sectors could be around 300,000 in 2015, that is just the double from the previous year and causing havoc in the financial space, security establishment, and social fabric.[3]Interestingly, Andhra Pradesh, Karnataka and Maharashtra, have ben raked top 3 state with highest online fraud, together contribute more than 70 per cent to India's revenue from IT and IT related industries[4].

The present study is based on secondary sources of data/ information. Different books, journals, newspapers and relevant websites have been consulted in order to make the study an effective one. The study attempts to examine the Impact and Importance of Cashless Transaction in India.

LITERATURE REVIEW

E-BANKING IN INDIAN BANKING SYSTEM

Enhanced role in the banking sector in the Indian economy, the increasing levels of deregulation and globalization in the Indian banking industry have placed numerous demands on the banks.

[2]India needs to spend $4 billion to combat cybercrime: Study, (Apr.13.2016)http://www.gadgetsnow.com/tech-news/India-needs-to-spend-4-billion-to-combat-cybercrime-ASSOCHAM-Mahindra-SSG-study/articleshow/51811417.cms

[3] ASSOCHAM-Mahindra SSG, Bank Fraud Was Waiting to Happen, (Oct 2016http://www.assocham.org/newsdetail.php?id=5995

[4]ASSOCHAM-CyberCrimesinIndiaislikelytocross300000by2015: Study, (Jan.04.2015,) http://www.assocham.org/newsdetail.php?id=4821

VOLUME 3 | JAN | 2018 ISSN: 2456-9704

To meet the varied needs of the customers, banks have to offer wider, flexible range of facilities tailored for all type of customers. Internet banking has changed a customer's behavior drastically due to the technological advancements. Use of financial services are today characterized by individuality, mobility, the interdependence of time and place.Internet is being used as a new distribution channel to provide complex products at owner costs to more and more potential customers. The Internet has helped banks to enlarge their market area without building new offices and to increase their market share and profits.

KINDS OF ONLINE FRAUDS

a) *Triangulation/site cloning*: Customers enter their card points of interest on fake shopping destinations. These points of interest are then abused.
b) *Hacking*: Hackers/fraudsters acquire unapproved access to the card administration stage of banking framework. Fake cards are then issued with the end goal of illegal tax avoidance.
c) *Online extortion*: Card data is stolen at the season of an online exchange. Fraudsters at that point utilize the card data to make online buys or expect a person's character.
d) *Lost/stolen card*: It alludes to the utilization of a card lost by an honest to goodness account holder for unapproved/unlawful purposes. Check card skimming: A machine or camera is introduced at an ATM so as to get card data and PIN numbers at the point when clients utilize their cards.
e) *ATM extortion*: A fraudster gains a client's card as well as PIN, what's more, pulls back cash from the machine.
f) *Social building*: A hoodlum can persuade a worker that he should be let into the workplace building, or he can persuade somebody via telephone or by means of email that he should get certain data.
g) *Dumpster jumping*: Employees who aren't watchful while tossing away papers containing touchy data may make a mystery information accessible to the individuals who check the organization's junk.
h) *False affectations*: Someone with the purpose to take corporate data can land a position with a cleaning organization or another merchant particularly to increase true blue access to the workplace building.
i) *Computer infections*: With each tap on the web, an organization's frameworks are interested in the danger of being tainted with accursed programming that is set up to reap data from the organization servers.

RISKS INVOLVED

In case of e-banking nothing is secure, use of high technology has brought the operational risk in the form of security risk not only in

the world but in India also cyber fraud has increased manifolds. Customer fear that their money can be targeted by the cyber frauds. In the environment of large scale use of technology, there is a need of surveillance monitoring and auditing to detect unusual usage pattern and deficiencies. This calls for putting in place appropriate and adequate safeguards to ensure security covering physical and other aspects[5]

LIMITATION TO E-BANKING

It pre-supposes computer literate customers who can develop trust in this technology which is not always the case especially, in a country like where literacy ratio is so less, it is not a very good idea to expect most of its population to support idea of cashless economy.

RESPONSIBILITIES AND LIABILITIES OF BANKS

Now days, most banking functions have moved to core banking system and a large number of transactions are made using internet banking, mobile banking or use of debit/credit cards. This research focuses on questions such as, "What happens when the bank or other intermediaries like telecom companies fails to provide adequate security measures to protect the customer from illegal and fraudulent transfers?"or, "What are the consequences when there is a lapse of care on the part of the banks and other intermediaries during such fraudulent transaction?".

Generally, intermediaries are not liable for the offence committed by the users or third parties using their network or system. However, they might be liable for non-compliance of due diligence requirements under the law If due to negligence of the body corporate in handling such sensitive personal data causes wrongful loss to such person, the body corporate is liable to pay adequate damages as compensation to such person.The banks are in possession of sensitive personal information of their customers including account numbers, PIN, credit/debit card numbers and other financial information of the customer in an electronic form. The banks are responsible for protection of such information from unauthorized usage through maintaining reasonable security procedures laid down in different rules and regulationsissued by RBI and other bodies. Some of the important rules and guidelines which govern maintenance of reasonable security standards for banks include, Master Circular

[5] Jyotsna Sethi & Nishwan Bhatia, Elements of Banking and Insurance, Phi learning private limited 65,66 (2nd ed. 2012)

– Know your Customer (KYC) norms, Anti-Money Laundering standards, Combating of financial terrorism, Obligations of banks under Protection of Money Laundering Act, 2002 and by RBI and other international standards for information technology security (ISO standards).

BREACH IN DATA SECURITY: WHY DOES IT OCCUR?

Some of the common breaches in security procedures by banks and telecom operators include:

- Non-compliance of KYC norms of customers by banks. Most of the proceeds of the fraudulent transactions are transferred either in "mule accounts" (accounts of innocent persons are used to transfer money in promise of payment of a certain percentage) or in accounts where the identity of the customers cannot be verified. Such accounts are generally created by using either apparently fraudulent documents or no proper documents as such.
- Non-compliance of KYC norms by the telecom operators while issuance of duplicate SIM card. In a large number of cases, the fraudster has obtained a duplicate SIM card of the victim's mobile, which was later used to receive one-time password or make mobile banking transaction, hencevictim's original SIM will get disabled and he will not be able to receive transaction messages.
- Non installation of CCTVs or non-working of CCTVs in banks, ATMs which is a necessary security procedure for banks.
- No mechanism to identify and flag suspicious transaction patterns.
- Failure to notify the customer of suspicious transactions (either through SMS or email) on a live basis

LEGISLATTIVE CHECK

INFORMATION TECHNOLOGY ACT 2000

a) Section 72 of The Information Technology Act, 2000 casts an obligation of confidentiality against the disclosure of any electronic record, register, correspondence and information, except for certain purposes and violation of this provisions is a criminal offense

b) Section 46 of the actprovides that, one can file an application before the Adjudicating Officer appointed claiming breach of reasonable security procedures by the bank. An analysis of selected cases ordered by the Adjudicating Officer in the state of Maharashtra revealed that the banks and telecom operators in most cases have failed to maintain reasonable security procedures, including non-compliance of KYC norms, Anti-money laundering guidelines, and automatic suspicious transaction monitoring facilities.

c) Section 43 of The Information Technology Act, 2000 provides

that the banks and other intermediaries who have failed to maintain reasonable security procedure must pay adequate damages as compensation to such person to cover the loss. The Adjudicating Officer has the power to adjudicate in the matters where the claim does not exceed Rs.5 crores. The bank must prove that they have maintained reasonable security procedures to prevent such fraudulent acts. In case the bank fails to prove that they have maintained reasonable security procedure, the Adjudicating Officer who has the powers of a Civil Court, may order the bank to pay damages as compensation to the victim.

STEPS TAKEN BY GOVERNMENT TO TACKLE ONLINE FRAUDS

ROLE OF RBI

Considering the scope of fraud in the electronic banking area and thepossibility of the contagion-Reserve bank of India as a regulator and a supervisor has been proactive in addressing the risks associated with the electronicbanking.The RBI has been promptly addressing issues relating to fraud with the use ofelectronic banking facilities. Even after issuing guidelines for a secured electronic banking, the RBI advises the banks, from time to time, on control mechanism,s to combat such frauds.Financial cybercrime in India has been steadily increasing over the years. For the year 2015-16, the Reserve Bank of India (RBI) reported 16,468 cyber crimes related to ATM, debit card, credit card and net banking frauds. The number of frauds reported by the RBI were 13,083 in the year 2014-15 and 9,500 in the year 2013-14.

Some of the measures taken by the Apex institution to tackle the current problems faced by the banking sectors are:

1) ***Re-BIT***

RBI has set up an entity called,'Re-BIT' known as Reserve Bank Information Technology Private limited. It tends to focus on IT and cyber security and also indulge in assessment of RBI regulated entities and assist in IT system audits, it would also work on implementing and managing internal or system wide IT assignments.

2) ***Customer Protection Circular***

Recently in August 2017, RBI has passed a circular releasing some guidelines to curb the increasing online frauds due to the Increased thrust on financial inclusion and customer protection and considering the recent surge in customer grievances relating to

unauthorized transactions[6], in this circular following guidelines have been given:

2.1) *Zero liability of a customer*: there will be zero liability o customer in case of third party breach where neither the fault is of customer or bank but of the system. However, the customer needs to notify the bank within 3 working days of receiving the communication from the bank regarding the unauthorized transaction.

2.2) *Reported in 7 days*: In case the fraud is reported within four to seven working days, a customer's maximum liability will be from Rs. 5,000 to Rs. 25000, depending on the type of accounts and credit card limit.

2.3) *When reported beyond 7 days*: the customer's liability will be according to the bank's policy. Banks have been asked to clearly define the rights and obligations of customers in case of unauthorized transactions in specified scenarios.

2.4) *Burden of proof*: The burden of proving customer liability in case of unauthorized electronic banking transactions shall lie on the bank.

2.5) *Limited Liability of customer*: On being notified by the customer, the bank has to credit the amount involved in the unauthorized electronic transaction to the customer's account within 10 working days from the date of such notification by the customer

2.6) *Mobile Registration Mandatory*: To safeguard customers from online frauds, banks have to ask their customers to mandatorily register for SMS alerts and wherever available register for e-mail alerts, for electronic banking transactions.

2.7) Such SMS/email alerts also must have a "Reply" option for customer response so that they can easily notify banks in case of fraudulent transactions.

2.8) According to the RBI directive, banks have to provide a direct link on their website's home page for lodging the complaints.

3) CERT(Computer Emergency Response Team):

Ministry of Electronics and Information Technology, issued a consultation paper which envisages development of a frameworkfor digital security that are operating in country. As part of the guidelines recommended, the government's has created CERT designated under Section 70B of Information Technology (Amendment) Act 2008 to serve as

[6]Reuters, RBI to limit customer liability in the wake of increased digital fraud, (May.31.2017) http://gadgets.ndtv.com/internet/news/rbi-to-limit-customer-liability-in-wake-of-increased-digital-fraud-1706323

the national agency to perform the following functions in the area of cyber security:

1. Collection, analysis and dissemination of information on cyber incidents
2. Forecast and alerts of cyber security incidents
3. Emergency measures for handling cyber security incidents
4. Coordination of cyber incident response activities
5. Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents[7]

DEFECTS IN CIRCULAR

There lies a lacuna regarding the Indiansectors of bankers who will be availing these facilities as:

- Firstly, the RBI mentions that "when a customer suffers a loss due to her negligence, she shall bear the entire loss until she reports the unauthorized transaction to the bank." This could be problematic because in many online frauds the customer would not even receive a notification for her transaction and could be unaware about it for a long time.
- Secondly Illiterates and those with limited knowledge of banking facilities in rural areas wouldn't be able to even identify an online fraud.
- Thirdly, the RBI limited the liability of the bank in case of breach by a third party. If a customer fails to report an unauthorized online transaction on his account to the bank within seven working days, then she is entitled to no more than Rs 5000 as compensation irrespective of her loss. In case the customer takes more than seven days to report the fraud, then the bank is under no liability to compensate her.

NEED FOR AWARENESS

Requirement for carefulness in the cyber world has been highlighted by many scholars. These frauds have picked up consideration resulting to the notice of demonetization, with rising digital managing an account exchanges and a legislative push towards a computerized economy. A few new issues originating from the doubt in computerized installment frameworks have been reported. For example, the cybercrime cell of the Mumbai Police has gotten a few reports of a trick portrayed by people accepting fraudulent calls

[7] Ministry of Technology and Information Act (Sep.15.2017, 2:28 am) http://meity.gov.in/content/icert

professedly from banks, talking about another RBI strategy. These calls educated shoppers that credit and check cards were destined to be deactivated, yet in the event that they discharged their card points of interest, they would be allowed to proceed with utilization.There has likewise been a rise in Ransom ware attacks recently, with more than 11,000 assaults being accounted for in only three months. This is notwithstanding the reality that 80% ofcybercrimes remain unreported according to late news reports. This post will audit a few activities taken towards the more effective examination of cybercrime by law authorization the nation over.[8]

CYBER POLICING IN INDIA

1) *CRIME AND CRIMINAL TRACKING NETWORK AND SYSTEMS (CCTNS):* CCTNS, a project running under the national e-governance plan, that has been approved by the cabinet committee on economic affair in the year 2009, It aims at creating a nationwide networking infrastructure for an IT-enabled criminal tracking and crime detection system. The integration of about 15,000 police stations, district and state police headquarters and automated services was originally scheduled to be completed by 2012. However, this still remains incomplete.
2) 'Centre Citizen Portal' - *ONLINE COMPLAINTS PORTAL:* As a response to the queries asked by Supreme Court on the measures taken to curb cybercrime, an online portal has been set up by central government called 'Centre Citizen Portal'. It allows the citizens to file any sort of complaints which may include cyber stalking, online financial fraud. This portal on receiving any such portal will trigger an alert to the police station and allow the police to track and update the status of the complaint and the complainant shall be able to view updates and escalate the complain to superior authority.
3) *CYBER POLICE STATIONS: Cyber police headquarters include trained staff and proper equipment to break down and track advanced crimes. As per a standing order of the DG and IGP of Bengaluru City Police issued in June 2016, where damage is of over INR 5 lakh can be enlisted at cyber police headquarters in instances of bank fraud. In instances of internet*

[8]Law and enforcement initiatives towards tackling cybercrime in India: CCG NLU, (Mar. 31. 2017 6:23 pm) https://www.medianama.com/2017/03/223-cybercrime-law-enforcement/

deceiving, just those cases where damage is over INR 50 lakh are reportedto jurisdiction of cyber police headquarters. All other case is to be enrolled with the nearby police headquarters which, dissimilar to cyber police headquarters, which unlike cyber cell do not include, proper gear to investigate and track digital crime.

4) *PREDICTIVE POLICING:* It involves the usage of data mining, statistical modeling and machine learning on datasets relating to crimes to make predictions about likely locations for police intervention. In 2013, Jharkhand Police, in collaboration with the National Informatics Centre, began developing a data mining software for scanning online records to study crime trends.

CHALLENGES FACED

BANKING SECTORIN INDIA

In India, legal infrastructure for promoting internet banking has not yet been put in place in a comprehensive manner. Banking Sector faces many challenges while executing policies among the customers:

1) India does not have licensed certifying authority appointed by the controller of certifying authorities to issue digital Signature certificates. India is not yet a signatory to the International Cyber Crime Treaty, which seeks to intensify cooperation among different signatory nations for exchanging information concerning cyber criminals.
2) There are unresolved legislative issues related to cyber crime laws, clarification regarding regulatory authority over e-money products, consumer protection and privacy laws. To make the electronic banking operation in India more widespread, secure and effective, these issues need to be addressed by relevant authorities[9].
3) As the banking practices and legislations concerning electronic banking are still in process of evolution in India and abroad because of technological innovations, there is a need for constant review of the current existing legislation in the banking sector.
4) The RBI is monitoring and reviewing legal and other requirements of electronic banking on a continuous basis to ensure that the e-banking would develop on sound lines and the e-banking would not pose a threat to financial stability.

LAW AND ENFORCEMENT

[9] S.M. Jawed Akhtar & Md. Shabbier Alam, Banking system in India: Reforms and Performance Evaluation, New Century Publication,170 (2011)

1) No formal technical knowledge on how to deal with the internet fraud cases. This is one of the main problem that occurs while execution of the laws made.
2) Struggling to establish the chain of evidence, as there is no visible evidence to start with. Online frauds are done on machines; it is very easy to erase all history leaving no evidence behind.
3) Lack of Cyber forensic knowledge, India is developing country where computers are a recent introduction, thus majority deals with lack of computer knowledge.
4) How to setup the action plan for investigation? Police and legislature makers are not capable enough to decide modus operandi to tackle the issue due to the lack of cyber knowledge.

RECOMMENDATIONS

To reduce the risk in frauds in online transactions, banks should have a security policy duly approved by the board of directors.They should also introduce logical access control to data, system, application, software, utilities, etc.at the minimum they should use the firewall system so that there is no direct connection between internet and bank's system. **Bankway** and **Flexcube** are the most popular e-banking solution used for securing electronic transactions in India.Biometrics which is the science of identifying an individual by means of personal characteristics like face, finger prints retina or voice, is another security paradigm which can empower banks to verify the actual identity of a person rather than merely depending upon a PIN number.

Banks should also ensure that the product that they offer should be restricted to account holders only and services shall include only local currency products.Any breach of security system shall be reported immediately to RBI, banks should make mandatory disclosures of risks, responsibilities and liabilities of the customers in doing business through the internet. It will be naive to assume that in e-banking there are only transactions risks. This is because transactional risk will give rise to legal issues and ultimately all these will have a monetary implication of its population reputation of the bank and trust in the entire financial system.

CONCLUSION

Cyber crimes are very common and criminals are using very sophisticated tools to commit the crime. Cyber criminals are taking advantage of peoples having less awareness about the Spam messages, Phishing mails from where they can steal the required information. Bank Frauds constitute a significant level of

cubicle offenses being examined by the police. Unlike other fruads these fruads constitute sum of lakhs and crores of rupees. Bank fraud is an criminal offence in numerous nations, characterized as wanting to acquire property or cash from any governmentally guaranteed budgetary organization. It is in some cases considered a white collar crime. It in expanding with the progression of time. All the major operational zones in keeping money speak to a decent open door for fraudsters with developing frequency being accounted for under store, advance and between branch bookkeeping exchanges, including settlements.

There is a need to track such activities by incorporating the SPAM filter, Phishing filter in web browser itself. Also banking organizations should take the step forward to educate the user, make them aware about the probable threats to his money through net banking.[10] Current control mechanism is not appropriate and not able to serve the purpose of curbing the online frauds thus many changes are need to be made in the same.

[10]P.S. Lokhande&Dr. B.B. Meshram, Collecting Digital Evidence: Internet Banking Fraud - Case study (Sep. 14.2017, 5:14pm), https://www.irjet.net/archives/V2/i2/Irjet-v2i2194.pdf