CHAPTER - III
CHAPTER-III

LEGAL PROBLEMS TO CONTROL CYBER CRIMES AGAINST E-BANKING IN INDIA.

The Narasimham Committee deserves mention in that it was instrumental in forcing Indian banks to become competitive. Fleet footed private sector banks, forced the public sector banks to embrace technology and improve their level of customer service. Next, the Khan Committee was highly important in that it recommended the setting up of universal banks. But most importantly, the Verma Committee recommended the need for greater use of IT even in the weak Public sector banks. Actually, the nationalization of banks back in the 80s is proving to be a major obstacle in bringing about the required technological changes.

The ICICI Bank kicked off online banking in 1996, followed by a host of other banks. But even for the Internet as a whole, 1996 to 1998 marked the adoption phase, while usage increased only in 1999, owing to lower ISP online charges, increased PC penetration and a tech-friendly atmosphere. On the other hand, the Public Sector Banks (PSUs) lagged in the race for adopting Internet banking practices. While, among the PSUs, the State Bank of India took the lead, others are yet to catch up on Internet banking services. Some banks blame it on the lack of regulations and procedures to go online. But, not many are willing to buy the argument. More than a lack of regulatory framework, it is a lack of zeal and a mindset in tune towards resisting any new technology that is holding back the nationalized banks.

Internet banking is an extension of traditional banking services. However, there are several instances, which contradict the legal framework for internet banking in India: Banking Regulations Act, 1949, the Reserve Bank of India Act, 1934 and the Foreign Exchange Management Act, 1999.
Information Technology solutions have paved a way to a new world of internet, business networking and e-banking, budding as a solution to reduce costs, change the sophisticated economic affairs to more easier, speedy, efficient, and time saving method of transactions. Various criminals like hackers, crackers have been able to pave their way to interfere with the internet accounts through various techniques like hacking the Domain Name Server (DNS), Internet Provider’s (IP) address, spoofing, phishing, internet phishing etc. and have been successful in gaining “un authorised access” to the user’s computer system and stolen useful data to gain huge profits from customer’s accounts.

Intentional use of information technology by cyber terrorists for producing destructive and harmful effects to tangible and intangible property of others is called “cyber crime”. Cyber crime is clearly an international problem with no national boundaries. Hacking attacks can be launched from any corner of the world without any fear of being traced or prosecuted easily. Cyber terrorist can collapse the economic structure of a country from a place where that country might not have any arrangements like “extradition treaty” to deal with that criminal. The only safeguard would be better technology to combat such technology already evolved and known to the Hackers. But that still has threat of being taken over by the intellect computer criminals.

To meet the challenges of cyber crime and to curb the threat, the Information Technology Act 2000 was enacted on 17 Oct 2000, to address a number of e-commerce regulatory issues after the United Nation General Assembly Resolution A/RES/51/162, dated the 30th January, 1997 by adopting the Model Law on Electronic Commerce adopted by the United Nations Commission.

This chapter contributes an understanding of the effects of negative use of Information technology, and how far the present law in India is successful in dealing with the issue, and what way is the legal structure lagging to curb the crime. Possible changes needed in the system and the ways to combat cyber terrorism having safe and trustworthy transactions.
3.1 FINANCIAL SECTOR REFORM IN INDIAN BANKING

3.1. FINANCIAL SECTOR REFORMS IN INDIAN BANKING
The financial sector reforms started in 1991 had provided the necessary platform for the banking sector to operate on the basis of operational flexibility and functional autonomy; enhancing productivity, efficiency and profitability.

The first phase of reforms were implemented in the backdrop of the report of The Committee on Financial System, 1992 (Chairman: M. Narasimham widely known as Narasimham Committee-I).

Further, the second phase of reforms was implemented as per the recommendations of the Committee on Banking Sector Reforms 1998 (Chairman: M. Narasimham popularly known Narasimham Committee II).

Banking sector reforms since 1991 are as under:-
1. Granting operational autonomy to banks.
2. Liberalization of entry norms for banks.
3. Reduction in statutory pre-emptions so as to release greater funds for commercial lending.
4. Deregulation of interest rates.
5. Relaxation in investment norms for banks.
6. Easing of restrictions in respect of banks' foreign currency investments.
7. Withdrawal of reserve requirements on inter-bank borrowings.

3.1.1 INITIATIVE OF RBI ON FINANCIAL SECTOR REFORMS
The RBI adopted a comprehensive approach on the reforms of the financial sector after following the Report of the Narasimham Committee, The Department of Supervision (DoS), now called Department of Banking Supervision (DBS) was set up within the RBI in 1993 to strengthen the institutional framework. A high powered Board for Financial Supervision (BFS), comprising the Governor of RBI as Chairman, one of the Deputy Governors as Vice-Chairman and four Directors of the Central Board of the RBI as members was constituted in November 1994. Measures such as deregulation of interest
rates, reduction of statutory pre-emption such as CRR and SLR, and provision of operational autonomy to the banks were taken to straighten the banks.  

**Working Group to Review the System of On-site Supervision over Banks (Chairman: S.Padmanabhan) was appointed in 1995.**

Apart from on-site inspections, the RBI has adopted three other supervisory approaches, viz. offsite monitoring, internal control system in banks and use of external auditors.

RBI adopted the internationally adopted capital adequacy, asset quality, management, earnings, liquidity and system, (CAMELS) rating 'model with systems and controls added to it for Indian banks and for foreign banks on CACS model (capital adequacy, asset quality, compliance, systems and controls). Consequently, examination of liquidity was added to make the model as CALCS.

**The Off-site Monitoring and Surveillance (OSMOS) system was implemented in 1995** as a part of crisis management framework for early warning system and as a trigger for on-site inspections of vulnerable institutions.

The banks were instructed to increase the level of utilization of the INFINET for regulatory-cum-supervisory reporting. In order to strengthen the banking system, it was considered necessary to introduce capital adequacy norms to ensure uniform standards of capital structure and progress towards **Basel Committee norms (Basel I).**

**The Basel II framework** has been designed to provide operations to banking system for determining the capital requirements for credit risk, market risk and operational risk and enable banks/supervisors to select approaches that are most appropriate for their operations and financial markets. Now Indian Banking System is at the verge of operationalisation of **Basel III framework.**

**Adoption of Information Technology in Banking Sector**

RBI had constituted various committees to work on adoption of Information Technology in banking sector. The reports of various committees are summed up in brief as under

---

238 IBA Bulletin (Various issues)
239 Reserve Bank of India, RBI Bulletin (Various issues)
1) Dr. C. Rangarajan Committee [1983]\textsuperscript{240}

\textbf{(A committee constituted for Mechanisation in Banking Industry)}

The committee in its report in 1984 recommended introduction of Computerisation and Mechanisation at branch, regional office / zonal office and head office levels of banks.

2) Dr. C. Rangarajan Committee [1988]\textsuperscript{241}

\textbf{(A committee was constituted for Computerisation in Banking Industry)}

The report acknowledged the purpose of computerisation for enhancement in customer service, decision making, housekeeping and profitability in banking industry. As per the observation of the committee, banking is a service industry and enhanced efficiency will show the way to rapid rate of growth in productivity of the staff and help to increase employment versatile. The employees in the banking industry should view computerisation as an instrument to enhance customer service and welcome it in letter and spirit.

3) W.S. Saraf Committee [1994]\textsuperscript{242}

\textbf{(A committee was constituted for technology issue in the banking industry)}

The committee examined technological issues related to the payment system and to make suggestion for widening the use of modern technology in the banking industry. The Saraf committee recommended to set up institutions for Electronic Funds Transfer system in India. The committee also analyses the use of BANKNET and optimum utilization of SWIFT by the banks in India.

4) Shere Committee [1995]\textsuperscript{243}

\textbf{(A committee was constituted to study the aspects relating to EFT System)}

The Shere committee had proposed framing of RBI (EFT system) regulations under section 58 of the Reserve bank of India Act 1934 (RBI Act.), amendments to the RBI act and to the bankers book evidence act, 1891 as short term measures and enacting of a few new acts such as EFT act, the computer misuse and data protection act etc. as long term measures. For the present situation this report is proved to be very useful and is

\textsuperscript{241} Reserve Bank of India (1989) Report of the committee on computerisation in banks (The Rangarajan committee) Mumbai:
\textsuperscript{242} www.rbi.com
\textsuperscript{243} www.Banknetindia.com
up to the mark. But if we want to develop more technology then another forward look on regulation is must. Even though we were having a good report with us but still certain loopholes like there is no specification related to security and regulatory provisions, training the police personnel related to Hi-tech banking crime and its investigations. The laws to amend up to, which extent etc. can be seen in the regulatory provisions and frauds are increasing day by day and we are not in a position to curb that crime immediately.

5) Narasimham Committee [1998][244]
(A committee was constituted for the up gradation of technology)
The committee has also emphasized need on the following issues:-
• Encryption on Public Switching Telephone Network (PSTN) lines
• Admission of electronic files as evidence
• Treating EFT on par with crossed cheques / drafts for purposes of Income Tax
• Electronic Record keeping
• Provide data protection
• Implementation of digital signatures
• Clarification on payment finality in case of EFT

3.1.2 INTERNET BANKING – A NEW MEDIUM
Internet in India is growing rapidly. It has given rise to new opportunities in every field we can think of, be it entertainment, business, sports or education. Internet also has its own disadvantages. One of the major disadvantages is Cybercrime – illegal activity committed on the internet..

3.1.2(A) BANKING TRANSACTIONS THROUGH INTERNET
In more recent times, it has been transformed by the internet– a new delivery channel that has facilitated banking transactions for both customers and banks.

244 RBI (1998) Report of the committee on Banking sector reforms (The Narasimham committee) : RBI Mumbai
### Table 3.1 - Internet Users and Population Statistics India, Asia & Rest of the World

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>India</td>
<td>1,205,073,612</td>
<td>5,000,000</td>
<td>167,335,676</td>
<td>11.4 %</td>
<td>11.4 %</td>
<td>62,713</td>
</tr>
<tr>
<td>Africa</td>
<td>1,073,380,925</td>
<td>4,514,400</td>
<td>167,335,676</td>
<td>15.6 %</td>
<td>3,606.7 %</td>
<td>7.0 %</td>
</tr>
<tr>
<td>Asia</td>
<td>3,922,066,987</td>
<td>114,304,000</td>
<td>1,076,681,059</td>
<td>27.5 %</td>
<td>841.9 %</td>
<td>44.8 %</td>
</tr>
<tr>
<td>Europe</td>
<td>820,918,446</td>
<td>105,096,093</td>
<td>518,512,109</td>
<td>63.2 %</td>
<td>393.4 %</td>
<td>21.5 %</td>
</tr>
<tr>
<td>Middle East</td>
<td>223,608,203</td>
<td>3,284,800</td>
<td>273,785,413</td>
<td>78.6 %</td>
<td>153.3 %</td>
<td>11.4 %</td>
</tr>
<tr>
<td>North America</td>
<td>348,280,154</td>
<td>108,096,800</td>
<td>254,915,745</td>
<td>42.9 %</td>
<td>1,310.8 %</td>
<td>10.6 %</td>
</tr>
<tr>
<td>Latin America</td>
<td>593,688,638</td>
<td>18,068,919</td>
<td>24,287,919</td>
<td>67.6 %</td>
<td>218.7 %</td>
<td>1.0 %</td>
</tr>
<tr>
<td>Australia</td>
<td>35,903,569</td>
<td>7,620,480</td>
<td>24,287,919</td>
<td>67.6 %</td>
<td>218.7 %</td>
<td>1.0 %</td>
</tr>
<tr>
<td>WORLD TOTAL</td>
<td>7,017,846,922</td>
<td>360,985,492</td>
<td>2,405,518,376</td>
<td>34.3 %</td>
<td>566.4 %</td>
<td>100.0 %</td>
</tr>
</tbody>
</table>

3.1.2(B) No. of Bank Branches & ATMs in India as on 31st March-2013

Table 3.2 - No. of Bank Branches & ATMs in India as on 31st March-2013

<table>
<thead>
<tr>
<th>S.N.</th>
<th>Types of the Banks</th>
<th>Total Branches</th>
<th>ATMs</th>
<th>On-site ATMs</th>
<th>Off-site ATMs</th>
<th>Total ATMs</th>
<th>% of Off-site to total ATMs</th>
<th>% of Off-site to total Branches</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. (A+B+C)</td>
<td>Schedule Commercial Banks</td>
<td>81,240</td>
<td>47,545</td>
<td>48,141</td>
<td>95,686</td>
<td>49.69%</td>
<td>50.31%</td>
<td></td>
</tr>
<tr>
<td>A) (a+b)</td>
<td>Public Sector Banks</td>
<td>67,466</td>
<td>34,012</td>
<td>24,181</td>
<td>58,193</td>
<td>58.45%</td>
<td>41.55%</td>
<td></td>
</tr>
<tr>
<td>a) Nationalised Banks</td>
<td>48,636</td>
<td>18,277</td>
<td>12,773</td>
<td>31,050</td>
<td>58.86%</td>
<td>41.14%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b) State Bank Group</td>
<td>18,830</td>
<td>15,735</td>
<td>11,408</td>
<td>27,143</td>
<td>57.97%</td>
<td>42.03%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B) Private Sector Banks</td>
<td>13,452</td>
<td>13,249</td>
<td>22,830</td>
<td>36,079</td>
<td>36.60%</td>
<td>63.40%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C) Foreign Banks</td>
<td>322</td>
<td>284</td>
<td>1,130</td>
<td>1,414</td>
<td>20.09%</td>
<td>79.91%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(A+B+C)Total</td>
<td>81,240</td>
<td>47,545</td>
<td>48,141</td>
<td>95,686</td>
<td>49.69%</td>
<td>50.31%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

245 India Internet and Telecommunications Reports
Source: http://www.internetworldstats.com/asia/in.htm#top#top

246 Trend & Progress in Banking 2010-11 RBI Annual Report
From the above table it reveals that total numbers of ATMs installed in India by various banks as on end March 2013 is 95,686. The Nationalised Bank having the largest numbers of ATMs i.e. 58,193 which is followed by State Bank Group i.e. 27,143 in the category of Public Sector Banks. Private Banks is having 22830 ATMs which are followed by Foreign Banks i.e. 1,414. While on site ATM is highest for the Nationalised banks of India.

The increasing use of technology, particularly by businesses to drive its operations and to deliver world class services has led to the evolution of a new threat. The growth of complexity and access to technology has made us more susceptible to ‘cyber crime’ which is also a new form of business threat that requires a fundamental shift in risk management arena of businesses, particularly in the financial domain where the risk is very high.

The Reserve Bank of India has taken several initiatives in setting guidelines for internet banking, and reviews them at periodic intervals. Most important, RBI approval was made mandatory for all banks before offering any transactional services over the Internet. This was however shelved, giving banks more autonomy on the online space, though ensuring at the same time, that it would be strictly under the provisions of the RBI.

3.1.2(C) TECHNOLOGY LEAD THE WAY FOR MOBILE BANKING

Due to invent of mobile phone technology almost every sector is using this new trend to lure more users. In this era of technology, banks are also in the race of persuading more customers to use their services. Largely, all banks are pushing ahead the idea of mobile banking to their customers after the introduction of electronic banking and considering modern day requirements.

<table>
<thead>
<tr>
<th>COUNTRY/YEAR</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>CAGR%</th>
</tr>
</thead>
<tbody>
<tr>
<td>BRAZIL</td>
<td>174.0</td>
<td>186.0</td>
<td>192.4</td>
<td>199.3</td>
<td>206.1</td>
<td>4.1</td>
</tr>
<tr>
<td>RUSSIA</td>
<td>174.3</td>
<td>181.2</td>
<td>186.6</td>
<td>191.5</td>
<td>195.8</td>
<td>2.8%</td>
</tr>
<tr>
<td>INDIA</td>
<td>525.2</td>
<td>604.1</td>
<td>666.0</td>
<td>723.1</td>
<td>787.4</td>
<td>10.2%</td>
</tr>
<tr>
<td>CHINA</td>
<td>747.4</td>
<td>855.8</td>
<td>963.6</td>
<td>1079.2</td>
<td>1200.1</td>
<td>11.9%</td>
</tr>
</tbody>
</table>

247 Source: www.eMarketer.com
3.1.2(D) MOBILE BANKING ON THE RISE IN INDIA

Increasing “Smart-Phone” adoption and initiatives such as media promotions and customer education programmes for mobile banking have led to this uptrend. For customers, mobile banking is convenient while banks benefit through a low-cost channel. For the country’s largest bank State Bank of India, of its total customer base of 200 million, about 5.2 million have registered for its mobile banking services. According to a KPMG report, with mobile Internet usage is expected to exceed desktop Internet use by 2014, mobile banking services will become even more important. It is particularly true of the Generation-Y group (18-32-year olds) who are three times more likely to adopt mobile banking than older users, the report said. Most big banks have seen a 100 per cent growth in mobile banking with more services waiting to be launched in the upcoming year. The Reserve Bank of India said, “The growth in mobile banking that has taken place in the country till date, though at a rapid pace, is yet to reach the critical mass that will enable it to deliver on its promise of reaching banking, including payment services, at a cheaper, secure and seamless manner to the existing and potential customers.” In private sector bank ICICI leads by 14.5 percent followed by Axis Bank with 9.4 per cent and Citi bank with 3.5 per cent. Around three per cent of SBI's total customer base is into mobile banking transactions. For ICICI Bank, over 10 million customers have currently registered for mobile banking.

Table 3.4- Data on Mobile Banking Share in Total Volume Terms (February to November 2012)\(^{248}\)

<table>
<thead>
<tr>
<th>Type of Bank/Month</th>
<th>Feb.</th>
<th>March</th>
<th>April</th>
<th>May</th>
<th>June</th>
<th>July</th>
<th>Aug</th>
<th>Sept</th>
<th>Oct</th>
<th>Nov.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Co-operative + Public Sector Banks</td>
<td>2.3</td>
<td>2.3</td>
<td>2.4</td>
<td>2.4</td>
<td>2.4</td>
<td>2.4</td>
<td>6.4</td>
<td>3.2</td>
<td>2.7</td>
<td>2.5</td>
</tr>
<tr>
<td>Private + Foreign Banks</td>
<td>12.1</td>
<td>13.7</td>
<td>14.4</td>
<td>18.4</td>
<td>20.6</td>
<td>21.1</td>
<td>22.5</td>
<td>24.3</td>
<td>27.7</td>
<td>30.1</td>
</tr>
<tr>
<td>State Bank Group</td>
<td>85.6</td>
<td>84.0</td>
<td>83.3</td>
<td>79.2</td>
<td>77.1</td>
<td>76.5</td>
<td>71.1</td>
<td>72.6</td>
<td>69.9</td>
<td>67.4</td>
</tr>
</tbody>
</table>

The SBI group dominates this space in volume terms with an overall share of 67.4 per cent in total volumes. Private and foreign banks follow, with an overall share of 30.1 per cent in November.

\(^{248}\) Source: www.rbi.com
Table 3.5 - Data on Mobile Banking Share in Total Value Terms (February to November 2012)

<table>
<thead>
<tr>
<th>Type of Bank/Month</th>
<th>Feb.</th>
<th>March</th>
<th>April</th>
<th>May</th>
<th>June</th>
<th>July</th>
<th>Aug</th>
<th>Sept</th>
<th>Oct</th>
<th>Nov.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Co-operative + Public Sector Banks</td>
<td>3.7</td>
<td>3.5</td>
<td>4.0</td>
<td>3.9</td>
<td>3.9</td>
<td>3.9</td>
<td>6.4</td>
<td>3.2</td>
<td>2.7</td>
<td>2.5</td>
</tr>
<tr>
<td>Private + Foreign Banks</td>
<td>46.0</td>
<td>49.0</td>
<td>49.2</td>
<td>56.4</td>
<td>58.3</td>
<td>59.3</td>
<td>60.6</td>
<td>59.0</td>
<td>73.5</td>
<td>61.6</td>
</tr>
<tr>
<td>State Bank Group</td>
<td>50.3</td>
<td>47.5</td>
<td>46.8</td>
<td>39.7</td>
<td>37.8</td>
<td>36.8</td>
<td>35.4</td>
<td>37.0</td>
<td>23.9</td>
<td>34.5</td>
</tr>
</tbody>
</table>

Among banks, private & foreign banks leads the race with 61.6 per cent share in the total number of mobile transactions carried out in November, followed by State Bank Group Banks with 34.5 per cent share. However, the SBI group has a lower share in value terms compared to the private and foreign banks. "In an evolving market, which is in its nascent stage, these developments are bound to happen when more banks get into the space," said an official from the bank.

**Banks permitted to provide Mobile Banking Service in India by RBI as appended below:**

**i) Twenty Nationalized Banks permitted for Mobile Banking Service – Position as on 08/07/2013**

Table 3.6 - Nationalised Banks permitted for providing mobile banking service

<table>
<thead>
<tr>
<th>1) Allahabad Bank</th>
<th>11) Indian Overseas Bank</th>
</tr>
</thead>
<tbody>
<tr>
<td>2) Andhra Bank</td>
<td>12) IDBI Bank</td>
</tr>
<tr>
<td>3) Bank of Baroda</td>
<td>13) Oriental Bank of Commerce</td>
</tr>
<tr>
<td>4) Bank of India</td>
<td>14) Punjab National Bank</td>
</tr>
<tr>
<td>5) Bank of Maharashtra</td>
<td>15) Punjab &amp; Sind Bank</td>
</tr>
<tr>
<td>6) Canara Bank</td>
<td>16) Syndicate Bank</td>
</tr>
<tr>
<td>7) Central Bank of India</td>
<td>17) UCO Bank</td>
</tr>
<tr>
<td>8) Corporation Bank</td>
<td>18) Union Bank of India,</td>
</tr>
<tr>
<td>9) Dena Bank</td>
<td>19) United Bank of India</td>
</tr>
<tr>
<td>10) Indian Bank</td>
<td>20) Vijaya Bank</td>
</tr>
</tbody>
</table>

249 Source: www.rbi.com
ii) Six Banks of State Bank Group permitted for Mobile Banking Service—Position as on 08/07/2013

<table>
<thead>
<tr>
<th>Table 3.7- State Bank Group permitted for Mobile Banking Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) State Bank of India</td>
</tr>
<tr>
<td>2) State Bank of Bikaner</td>
</tr>
<tr>
<td>3) State Bank of Hydrabad</td>
</tr>
<tr>
<td>4) State Bank of Mysore</td>
</tr>
<tr>
<td>5) State Bank of Patiyala</td>
</tr>
<tr>
<td>6) State Bank of Travancore</td>
</tr>
</tbody>
</table>

iii) Twenty Private Sector Banks permitted for Mobile Banking Service—Position as on 08/07/2013

<table>
<thead>
<tr>
<th>Table 3.8- Private Sector Banks permitted for Mobile Banking Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Axis Bank Ltd</td>
</tr>
<tr>
<td>2) Development Credit Bank</td>
</tr>
<tr>
<td>3) Dhanlaxmi Bank Ltd</td>
</tr>
<tr>
<td>4) The Federal Bank Limited</td>
</tr>
<tr>
<td>5) HDFC Bank Ltd</td>
</tr>
<tr>
<td>6) ICICI Bank Ltd</td>
</tr>
<tr>
<td>7) IndusInd Bank Ltd</td>
</tr>
<tr>
<td>8) Ing Vaisya Bank Ltd</td>
</tr>
<tr>
<td>9) Jammu &amp; Kashmir Bank</td>
</tr>
<tr>
<td>10) Karnataka Bank Ltd</td>
</tr>
<tr>
<td>11) Karur Vysya Bank Ltd</td>
</tr>
<tr>
<td>12) Kotak Mahindra Bank Ltd</td>
</tr>
<tr>
<td>13) Laxmi Vilas Bank Ltd</td>
</tr>
<tr>
<td>14) South Indian Bank Ltd</td>
</tr>
<tr>
<td>15) Tamilnad Mercantile Bank ,</td>
</tr>
<tr>
<td>16) Catholic Syrian Bank Ltd</td>
</tr>
<tr>
<td>17) City Union Bank Limited</td>
</tr>
<tr>
<td>18) The Nainital Bank Ltd</td>
</tr>
<tr>
<td>19) The Ratnakar Bank Ltd</td>
</tr>
<tr>
<td>20) Yes Bank Ltd</td>
</tr>
</tbody>
</table>

iv) Eleven Foreign Banks permitted for Mobile Banking Service—Position as on 08/07/2013

<table>
<thead>
<tr>
<th>Table 3.9- Foreign Banks permitted for Mobile Banking Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) BNP Paribas</td>
</tr>
<tr>
<td>2) Bank of America</td>
</tr>
<tr>
<td>3) Barclays Bank PLC</td>
</tr>
<tr>
<td>4) Citi Bank NA</td>
</tr>
<tr>
<td>5) Deutsche Bank AG</td>
</tr>
<tr>
<td>6) FirstRand Bank Ltd</td>
</tr>
<tr>
<td>7) JP Morgan Chase Bank NA</td>
</tr>
<tr>
<td>8) The Hong Kong and Shanghai Banking Corporation Ltd.</td>
</tr>
<tr>
<td>9) The Royal Bank of Scotland N.V</td>
</tr>
<tr>
<td>10) Standard Chartered Bank</td>
</tr>
<tr>
<td>11) The Development Bank of Singapore Limited</td>
</tr>
</tbody>
</table>

v) Nine Regional Rural Banks permitted for Mobile Banking Service—Position as on 08/07/2013

<table>
<thead>
<tr>
<th>Table 3.10- Regional Rural Banks permitted for Mobile Banking Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Baroda Gujarat Garmin Bank</td>
</tr>
<tr>
<td>2) Baroda Rajasthan Garmin Bank</td>
</tr>
<tr>
<td>3) Baroda U. P. Garmin Bank</td>
</tr>
<tr>
<td>4) Jhabua- Dhar Kshetriya Garmin Bank</td>
</tr>
<tr>
<td>5) Pallavan Grama Bank</td>
</tr>
<tr>
<td>6) Pragathi Garmin Bank</td>
</tr>
<tr>
<td>7) Shreyas Garmin Bank</td>
</tr>
<tr>
<td>8) South Malabar Garmin Bank</td>
</tr>
<tr>
<td>9) Uttarakhand Garmin Bank</td>
</tr>
<tr>
<td>10) Pragathi Garmin Bank</td>
</tr>
</tbody>
</table>

Table 3.11- Urban State & Dist. Central Cooperative Banks permitted for Mobile Banking Service

| 3) Bassein Catholic Co-op. Bank Ltd | 9) The Dombivli Nagar Sahakari Bank Ltd |
| 4) Janaseva Sahakari Bank Ltd | 10) The Cosmos Co-operative Bank Ltd |
| 5) Janata Sahakari Bank Ltd | 11) The Sarswat Co-operative Bank Ltd |
| 6) NKGSB Co-operative Bank Limited | 12) The Thane Janta Sahakari Bank Ltd |

Mobile banking is the future because of its cost effectiveness and ability to reach out to customers in remote areas. Banks will be able to approve and give loans via mobile banking. This will further reduce the need to go to a branch. Financial inclusion will be effectively done.
3.2 EXISTING LEGAL FRAMEWORK OF CYBER LAWS IN INDIA

Due to the dawn of Internet and its world wide acceptance by the people, the various countries in the world started enacting the cyber laws to control the cyber crime. As Internet transactions has started growing in India, the law enforcement agencies felt to enact the relevant Cyber laws which are necessary to control the cyber crimes in India. It was further decided to enact cyber laws in India to provide a sound legal framework to control the cyber crimes in India. In the year 2000, India enacted its first cyber law namely, the Information Technology Act, 2000. The IT Act, 2000 is based on the Model law of E-commerce adopted by UNCITRAL in 1996. The objective of the IT Act, 2000 is to provide legal recognition for transactions carried out through electronic means, to facilitate the electronic filing of documents with government agencies and to amend certain Acts i.e. the Indian Penal Code, 1860, Indian Evidence Act, 1872. The IT Act, 2000 gave the recognition to electronic and digital signature as well as to provide legal validity to electronic documents. IT Act also enabled the contracts in electronic form i.e. e-contracts legal, valid and enforceable. Information Technology Act also provides the legal remedy to control cyber crimes and to reprimand the miscreants.

The primary source of cyber law in India is the Information Technology Act, 2000 (IT Act) which came into force on 17 October 2000. With the passage of time, as technology developed further and new methods of committing crime using Internet & computers, the need was felt to amend the IT Act, 2000 to add new kinds of cyber offences and to remove loopholes in the existing Act which posed hurdles in the effective enforcement of the IT Act, 2000. This lead to the enactment of the Information Technology (Amendment) Act, 2008 which was made effective from 27 October 2009. The IT (Amendment) Act, 2008 has brought marked changes in the IT Act, 2000 on several counts.
3.2.1 DEVELOPMENTS IN INDIAN CYBER LAW AFTER THE ENACTMENT OF INFORMATION TECHNOLOGY ACT 2000

- On 17th October 2000, the *Information Technology (Certifying Authorities) Rules, 2000* also enacted. These rules stipulate the eligibility, appointment and working of Certifying Authorities. These rules also set down the technical standards, procedures and security methods to be used by a Certifying Authority.
- The *Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000* also enacted on 17th October 2000. These rules are related with the appointment and working of the Cyber Regulations Appellate Tribunal whose is responsible to hear appeals against orders of the Adjudicating Officers.
- Minor errors in the Act were rectified by the *Information Technology (Removal of Difficulties) Order, 2002* which was passed on 19 Sep. 2002.
- An *Executive Order* dated 12 September 2002 contained instructions relating provisions of the Act in regard to protected systems and application for the issue of a Digital Signature Certificate.
- The IT Act was amended by the *Negotiable Instruments (Amendments and Miscellaneous Provisions) Act, 2002*. This introduced the concept of electronic cheques and truncated cheques.
- *Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004* has provided the necessary legal framework for filing of documents with the Government as well as issue of licensees by the Government. It also provides for payment and receipt of fees in relation to the Government bodies.
- On the same day, the *Information Technology (Certifying Authorities) Rules, 2000* also came into force. These rules prescribe the eligibility, appointment and working of Certifying Authorities (CA). These rules also lay down the technical standards, procedures and security methods to be used by a CA. These rules were amended in 2003, 2004 and 2006.
Information Technology (Certifying Authority) Regulations, 2001 came into force on 9 July 2001. They provide further technical standards and procedures to be used by a CA.

Two important guidelines relating to CAs were issued. The first are the Guidelines for submission of application for license to operate as a Certifying Authority under the IT Act. These guidelines were issued on 9th July 2001.

Next were the Guidelines for submission of certificates and certification revocation lists to the Controller of Certifying Authorities for publishing in National Repository of Digital Certificates. These were issued on 16th December 2002.

The Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000 also came into force on 17th October 2000. These rules prescribe the appointment and working of the Cyber Regulations Appellate Tribunal (CRAT) whose primary role is to hear appeals against orders of the Adjudicating Officers.

Information Technology (Other powers of Civil Court vested in Cyber Appellate Tribunal) Rules 2003 provided some additional powers to the CRAT.

On 17th March 2003, the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 were passed. These rules prescribe the qualifications and experience of Adjudicating Officers, whose chief responsibility under the IT Act is to adjudicate on cases such as unauthorized access, unauthorized copying of data, spread of viruses, denial of service attacks, disruption of computers, computer manipulation etc. These rules also prescribe the manner and mode of inquiry and adjudication by these officers. The Information Technology (Security Procedure) Rules, 2004 came into force on 29th October 2004. They prescribe provisions relating to secure digital signatures and secure electronic records. Also relevant are the Information Technology (Other Standards) Rules, 2003.

An important order relating to blocking of websites was passed on 27th February, 2003. Computer Emergency Response Team (CERT-IND) can instruct Department of Telecommunications (DOT) to block a website\textsuperscript{250}.

\textsuperscript{250} Information Technology Act 2000
The Indian Penal Code is amended by the Information Technology Act to control various cyber crimes like forgery of electronic records, cyber frauds, destroying electronic evidence etc.

Indian Evidence Act is amended by the Information Technology Act to detect, to collect, to preserve and to prove the Digital Evidence in the court as per the provisions of the law.

Bankers' Book Evidence Act is amended by the Information Technology Act to make the provisions of this act relevant to digital bank records.

Code of Criminal Procedure is amended by the Information Technology Act in such an efficient manner to Investigate and adjudicate the cyber crimes in accordance with the provisions of the Information Technology Act.

Civil Procedure Code is amended by the Information Technology Act in such an efficient manner to Investigate and adjudicate the cyber crimes in accordance with the provisions of the Information Technology Act.

The Reserve Bank of India Act was also amended by the Information Technology Act.

3.2.2 THE MAJOR ACTS, AMENDED AFTER ENACTMENT OF IT ACT 2000

1) The Indian Penal Code, 1860
The Indian Penal Code was amended by inserting the word 'electronic' thereby treating the electronic records and documents on a par with physical records and documents. The Sections dealing with false entry in a record or false document etc (e.g. 192, 204, 463, 464, 464, 468 to 470, 471, 474, 476 etc) have since been amended as 'electronic record and electronic document' thereby bringing within the ambit of IPC. Now, electronic record and electronic documents has been treated just like physical records and documents during commission of acts of forgery or falsification of physical records in a crime. After the above amendment, the investigating agencies file the cases/charge-sheet quoting the relevant sections from IPC under section 463, 464, 468 and 469 read with the ITA/ITAA under Sections 43 and 66 in like offences to ensure the evidence and/or punishment can be covered and proved under either of these or under both legislation.
2) **The Indian Evidence Act 1872**

Prior to enactment of ITA, all evidences in a court were in the physical form only. After existence of ITA, the electronic records and documents were recognized. The definition part of Indian Evidence Act was amended as "all documents including electronic records" were substituted. Other words e.g. 'digital signature', 'electronic form', 'secure electronic record' 'information' as used in the ITA, were also inserted to make them part of the evidentiary importance under the Act. The important amendment was seen by admissibility of electronic records as evidence as enshrined in Section 65B of the Act assumes significance. This is a highly structured section and a milestone of legislation in the area of evidences produced from a computer or electronic device. Any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be treated like a document, without further proof or production of the original, if the conditions are satisfied as mentioned in the section.

3) **The Bankers' Books Evidence (BBE) Act 1891:**

Before passing of ITA, a bank was supposed to produce the original ledger or other physical register or document during evidence before a Court. After enactment of ITA, the definitions part of the BBE Act stood amended as: "bankers' books include ledgers, day-books, cashbooks, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device". When the books consist of printouts of data stored in a floppy, disc, tape etc, a printout of such entry certified in accordance with the provisions to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorized persons; the safeguards adopted to prevent and detect unauthorized change of data to retrieve data that is lost due to system failure. The above amendment in the provisions in Bankers Books Evidence Act recognized the printout from a computer system and other electronic document as a valid document during course of evidence, provided,
such print-out or electronic document is accompanied by a certificate in terms as mentioned above.

4) Amendment to the Reserve Bank of India Act, 1934 (2 of 1934)
The Reserve Bank of India Act, 1934 shall be amended in the manner specified in the Fourth Schedule to this Act.

Fourth Schedule of Information Technology Act, 2000
In the Reserve Bank of India Act, 1934, in section 58, in sub-section (2), after clause (p), the following clause shall be inserted, namely Clause (pp) the regulation of fund transfer through electronic means between the banks or between the banks and other financial institutions referred to in clause(c) of section 45-1, including the laying down of the conditions subject to which banks and other financial institutions shall participate in such fund transfers, the manner of such fund transfers and the rights and obligations of the participants in such fund transfers”.

5) Civil Procedure Code, 1908
The Cyber Appellate Tribunal has, for the purposes of discharging its functions under the IT Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908. However, is not bound by the procedure laid down by the Code of Civil Procedure, 1908 but is guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules. The Cyber Appellate Tribunal has powers to regulate its own procedure including the place at which it has its sitting.

6) Code of Criminal Procedure, 1973
Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.
3.2.3 RULES & NOTIFICATIONS ISSUES BY GOVERNMENT OF INDIA AFTER ENACTMENT OF IT ACT 2000

Controller of Certifying Authorities on behalf of Government of India, Ministry of Communications & Information Technology Department of Electronics & Information Technology, issued the various Rules & Notifications after enactment of Information Technology Act 2000

INFORMATION TECHNOLOGY RULES 251

Information technology act, 2000 provides the required legal sanctity to the digital signatures based on asymmetric crypto system. The digital signatures are now accepted at par with handwritten signatures and the electronic documents that have been digitally signed are treated at par with paper documents. The act provides the basic legal and administrative framework for e-commerce, and prompts its growth by creating trust in electronic environment. It is based on Model Law for e-commerce proposed by UNCITRAL with the following major concepts: Legal recognition of data messages, Writing Signature, Original, Admissibility and evidential weight of data message, retention of data message, Formation and validity of contracts, Recognition of parties by data message, Attribution of data message, Acknowledgement of receipt, Time and dispatch and receipt of messages.

1) INFORMATION TECHNOLOGY CERTIFYING AUTHORITY REGULATIONS, 2001 252

Controller of Certifying Authorities, Department of Information Technology, Ministry of Communications and Information Technology, under Section 89 of the IT Act 2000 issued July 9, 2001, Information Technology Certifying Authority Regulations, 2001 and published in official gazette. The rules are related terms and conditions of license to issue digital signature certificate.

251 Official Gazette of Govt. of India
252 Ibid
2) ORDER REGARDING THE APPOINTMENT OF ADJUDICATING OFFICERS [GSR 240(E)]

G.S.R.240(E) In exercise of the powers conferred by sub-section (1) of section 46 of the Information Technology Act, 2000 (21 of 2000), non 25th March, 2003 the Central Government hereby makes the following order/appointments viz. –

1. Whereas sub-section (1) of the section 46 makes provision for appointment of one or more Adjudicating Officers not below the rank of Director to the Central Government and subsection (3) requires that such an officer should possess experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government and whereas such experience necessary for appointment as Adjudicating Officer has been notified by the Central Government as per the Gazette Notification for Information Technology Rules 2003 under the short title Qualification and Experience of Adjudicating Officer and Manner of Holding Enquiry vide Gazette Notification GSR dated March, 2003.

2. Further Whereas the Secretary of the Department of Information Technology of each of the States or Union Territories are normally not below the rank of Director and possess the requisite experience in the field of Information Technology and also possess legal/judicial experience as required, therefore the Secretary of Department of Information Technology of each of the States or of Union Territories is hereby appointed as Adjudicating Officer for the purposes of the Information Technology Act, 2000.

3. The Department of Information Technology of each of the States or of Union Territories shall provide the infrastructure and maintain the records of the matters handled by Adjudicating Officer functioning in the States/Union Territories.
3) CYBER REGULATIONS APPELLATE TRIBUNAL (SALARY, ALLOWANCES AND OTHER TERMS AND CONDITIONS OF SERVICE OF PRESIDING OFFICER) RULES, 2003 [GSR 221(E)]

G.S.R.221 (E) In exercise of the powers conferred by clauses (r) of sub-section (2) of Section 87 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules regulating the terms and conditions of the service of the Presiding Officer, namely The Cyber Regulations Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Presiding Officer) Rules, 2003.

4) INFORMATION TECHNOLOGY (QUALIFICATION AND EXPERIENCE OF ADJUDICATING OFFICERS AND MANNER OF HOLDING ENQUIRY) RULES, 2003 [GSR 220(E)]

G.S.R.220(E):- In exercise of the powers conferred by Clauses (p) & (q) of subsection (2) of Section 87 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules namely:

(a) These rules may be called the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003.
(b) These shall come into force on the date of their publication in the Official Gazette.

5) INFORMATION TECHNOLOGY (QUALIFICATION AND EXPERIENCE OF ADJUDICATING OFFICERS AND MANNER OF HOLDING ENQUIRY) RULES, 2003 [GSR 220(E)]

G.S.R.220(E).--- In exercise of the powers conferred by Clauses (p) & (q) of subsection (2) of Section 87 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules on 17th March, 2003 namely

(a) These rules may be called the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003.
(b) These shall come into force on the date of their publication in the Official Gazette.

6) NOTIFICATION RELATED TO PERFORMANCE BOND IN THE FORM OF BANK GUARANTEE [GSR 902(E)]

In exercise of the powers conferred by section 87 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following amendments in the Information Technology (Certifying Authorities) Rules, 2000 on 21st November 2003 namely

(1) These rules may be called the Information Technology (Certifying Authorities) (Amendment) Rules, 2003.

(2) They shall come into force on the date of their publication in the Official Gazette.

7) APPLICATION FORM FOR ISSUE OF DIGITAL SIGNATURE CERTIFICATE FOR THE CATEGORY 'INDIVIDUAL' [GSR 285(E)]

GSR 285E,- In exercise of the powers conferred by section 87 of the information Technology Act 2000(21 of 2000), the Central Government hereby makes the following amendments in the IT Certifying Authority Rules notified vide Notification No GSR 789(E) dated 17.10.2000 vide which Application form for issue of Digital Signature Certificate for the category ‘Individual”.

8) INFORMATION TECHNOLOGY (OTHER STANDARDS), RULES 2003- (GSR 903(E) -STANDARDS TO BE OBSERVED BY THE CONTROLLER)

GSR 904(E),- In exercise of the powers conferred by clause (g) of subsection (2) of section 87 read with sub-section (2) of section 20 of the Information Technology Act,2000(21 of 2000), the Central Government hereby makes the following rules on 21st November 2003, namely:

(1) These rules may be called the Information Technology (Other Standard) Rules, 2003.

(2) They shall come into force on the date of their publication in the Official Gazette.

256 Official Gazette of Govt. of India
9) INFORMATION TECHNOLOGY (SECURITY PROCEDURE) RULES, 2004 [GSR 735(E)]
GSR 735(E),- In exercise of the powers conferred by clause (e) of subsection (2) of section 87 read with sub-section 16 of section 20 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules on 29th October 2003, namely:

(1) These rules may be called the Information Technology (Security Procedure) Rules, 2004.

(2) They shall come into force on the date of their publication in the Official Gazette.

10) ADDITIONS IN THE GSR 902(E), DATED 21-11-2003 [GSR 245(E)]
GSR 245(E),- In exercise of the powers conferred by section 87 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following addition in the G.S.R. 902(E) dated 21-11-2003:

Note:- The Principal Rules were published in Gazette of India, Extraordinary, Part II, Section 3, Sub-section (i) vide G.S.R. No. 788(E) dated 17-10-2000 and lastly amended vide G.S.R. No. 902(E), dated 21-11-2003 published in the Gazette of India, Extraordinary, Part II, Section 3, Sub-section (i).

11) Information Technology (Certifying Authorities) (Amendment) Rules, 2005 [GSR 32(E)]
GSR 32(E),- In exercise of the powers conferred by section 87 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following amendments on 18th January 2006 in the Information Technology (Certifying Authority) Rules, 2006, namely:

(1) These rules may be called the Information Technology (Certifying Authority) (Amendment) Rules, 2004.

(2) They shall come into force on the date of their publication in the Official Gazette.

\[257\] Official Gazette of Govt. of India
12) Instructions regarding applications of Section 35(3), Section 35(4) and Section 70(1) of Information Technology Act, 2000

Central Government herewith issues following instructions on 12th September 2002 for application of above three Sections: -

(i) For the purpose of sub-sections (3) and (4) of Section 35 of the Information Technology Act, 2000 (21 of 2000) hereinafter referred to on the said Act, every application for the issue of a Digital Signature Certificate shall not be required to be accompanied by a certificate practice statement as required under the said sub-sections.

(ii) For the purpose of sub-section 1 of Section 70 of the Act, details of every protected computer, computer system or computer network so notified by appropriate government may be informed to the Controller of Certifying Authorities, Department of Information Technology, 6 CGO Complex, New Delhi for the purpose of records and exercising powers under the said Act.

13) Information Technology (Certifying Authorities) (Amendment) Rules, 2009

[GSR 566(E)-Hash Algorithms]

GSR 566(E).- In exercise of the powers conferred by section 87 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules further to amend Information Technology (Certifying Authority) Rules, 2000, namely:

1. These rules may be called the Information Technology (Certifying Authority) (Amendment) Rules, 2009.

2. They shall come into force on the date of their publication in the Official Gazette. In Information Technology (Certifying Authorities) Rules, 2000, in rule 6 for the letters, figures and words “SHA-1 and SHA-2” shall be substituted

---

258 Official Gazette of Govt. of India
Information Technology (Certifying Authorities), Amendment Rules 2011-
25TH October 2011(Gsr 782(E) & Gsr 783(E)-Standards (Hash & Key Size), Usage Period Of Private Keys, Verification Of Digital Signature Certificate.

GSR 782(E).- In exercise of the powers conferred by section 87 of the Information Technology Act,2000(21 of 2000), the Central Government hereby makes the following rules further to amend Information Technology (Certifying Authority) Rules, 2000.namely:

(i) These rules may be called the Information Technology (Certifying Authority) (Amendment) Rules, 2011.

(ii) They shall come into force on the date of their publication in the Official Gazette.

In the Information Technology (Certifying Authority) Rules, 2000.

a) In rule 4, for the words “and the Digital Signature shall be attached to its electronic records” the word “the Digital Signature and the digital signature Certificate attached to its electronic record shall be stored or transmitted along with its electronic record” shall be substitute.

b) After rule 5, the following rules shall be inserted namely,

5A. Verification of Digital Signature Certificate:

a) The self signed certificate generated by the Controller, which begins the trust chain for the public key infrastructure shall be used to verify the authority of the public key certificate of the licensed Certifying Authorities.

b) The public key certificate of the licensed Certifying Authorities shall be used to verify the authenticity of the digital signature certificate issued to the subscribers.

c) The certificate revocation list maintained by the licensed Certifying Authorities shall be checked to confirm whether the certificate is valid or whether it has been revoked under section 38 of the act.

d) While verifying the validity of a digital signature the corresponding digital signature certificate should chain up through then public key certificate of the issuing Certifying Authority to the self signed certificate of the Controller and if

---

259 Official Gazette of Govt. of India
260 Official Gazette of Govt. of India
any of the certificates in the trust chain is not trusted the signature will not be verified.

GSR 783(E),—In exercise of the powers conferred by section 87 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules further to amend Information Technology (Certifying Authorities) Rules, 2000.namely:

(i) These rules may be called the Information Technology (Certifying Authorities) (Amendment) Rules, 2011.
(ii) They shall come into force on the date of their publication in the Official Gazette.

In the Information Technology (Certifying Authorities) Rules, 2000 (herein after referred to as the said rules), in rule 6,:—

a) For the letter, figure & words “SHA-1 and SHA-2” the letter, figure & word “SHA-2” shall be substituted.

b) For the figure & words “512,1024 &2048” the figure & word “2048 and 4096 bit” should be substituted

c) After, “Digital Signature Request Format PKCS#10” Following shall be inserted namely:

“Explanation-The Digital Signature Certificate granted before the commencement of the Information Technology (Certifying Authorities Amendment) Rules, 2011 using SHA-1, digital hash function standard shall continue to be valid till the date of expiry of such certificate.

In Schedule-III to the said rules, in the guidelines, for paragraph 21, the following paragraph shall be substituted namely:-

“21. Usage period for keys—

(1) Certifying Authority and subscriber shall be changed periodically

(2) Key change shall be processed as per Key Generation Guidelines

(3) The Certifying Authority shall provide reasonable notice to the Subscriber’s relying parties of any change to a new pair used by the Certifying Authority to sign Digital Signature Certificate
(4) All Certifying Authorities Key Pair and associate certificates must have validity period no more than 10 years
(5) All subscribers Key pairs and associated certificates must have validity period of no more than 3 years

3.2.4 NOTIFICATIONS

1) Notification no. G.S.R.240(E) dated 25.3.2003 regarding appointment of Secretary of the Department of Information Technology of each of the States or Union Territories as Adjudicating Officer

2) Notification no. G.S.R.221(E) dated 17.3.2003 regarding Cyber Regulations Appellate Tribunal (Salary, Allowances and other terms and conditions of Service of Presiding Officer) Rules 2003


4) Notification no. G.S.R.181(E) dated 27.2.2003 regarding establishment of Computer Emergency Response-in India (CERT-In) and the procedure for blocking of websites

5) Notification no. G.S.R.717(E) dated 22.10.2002 regarding Cyber Regulations Appellate Tribunal ( Salaries, allowances and other condition of service of other Officers and Employees) Rules, 2002


7) Notification G.S.R 904 (E) pertaining to the Information Technology (Other Standards) Rules, 2003

8) Notification G.S.R 903 (E) pertaining to the Information Technology ( other powers of Civil Court vested in Cyber Appellate Tribunal Rules, 2003

9) Notification G.S.R 902 (E) under Section 87 pertaining to the Information Technology (Certifying Authorities) ( Amendment ) Rules, 2003

10) Notification G.S.R 901 (E) under Section 87 (2) (s) pertaining to the Cyber Regulation Appellate Tribunal ( Procedure for investigation of misbehavior or incapacity of Presiding Officer) Rules, 2003
11) Different Opinion on the procedure to be followed for electronic filing of records under Section 87 (2) (b) and 87 (2) (c)


13) Notification No. 735(E) dated 29.10.2004 regarding Security Procedure for the purpose of creating Secure Electronic Record and Secure Digital Signature under Section 87(2)(e).

14) Notification No. 582 dated 6.9.2004 regarding use of electronic records and digital signatures under Section 87(2)(b)&(c)


16) Notification G.S.R 799 (E) pertaining to amendment in the Notification No. G.S.R 220 (E)

17) Gazette Notification G.S.R. 582(E) under Section 87 pertaining to rule under Section 87(2)(b) & (c) of the IT Act, 2000.


19) Information Technology (Certifying Authorities) Amendment Rules 2009(59KB)

20) G.S.R. 630(E) dated 26.7.2010 - Notification for declaring TETRA Secured Communication System Network of Govt. of NCT of Delhi as Protected System under section 70 of the IT Act, 2000

21) G.S.R. 410(E) dated 17.5.2010 - Notification for rescinding of earlier notifications G.S.R. 181(E) and G.S.R. 529(E)

22) S.O 117(E) dated 20.1.2010 --Notification for Designated Officer under section 69A and Rule 3 of Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public Rules, 2009

23) Notification of Rules under Section 52, 54, 69, 69A, 69B

24) Enforcement of IT (Amendment) Act 2008

27) GSR 313(E) Dated 11 April 2011: Information Technology (Reasonable Security Practices and procedures and sensitive personal data or information) Rules, 2011
29) G.S.R. 782(E) and G.S.R. 783(E) dated 25.10.2011 - Information Technology (Certifying Authorities) Amendment Rules, 2011
30) G.S.R. 153(E) Dated 16 march 2012 - Process of registration of cyber cafe to be followed by registration agency.
31) G.S.R 827(E) dated 16.11.2012 - Cyber Regulations Advisory Committee
32) Advisory to State/UT Govt. on implementation of Section 66A of the IT Act, 2000.
33) GSR 51(E) Dated 24 January 2013: Information Technology (Salary, Allowances and Terms and Conditions of Service of the Director General, Indian Computer Emergency Response Team) Rules, 2012
34) GSR 50(E) Dated 24 January 2013: Cyber Appellate Tribunal (Salary, Allowances and Other Terms and Conditions of Service of Chairperson and Members) Amendment Rules, 2012
35) Clarification on The Information Technology (Intermediary Guidelines) Rules, 2011

3.2.5. STRENGTH AND WEAKNESSES OF ITACT

Whatever stated in the foregoing paragraphs, it is clear that the IT Act 2000 tried to change outdated laws and pave the ways to combat with cyber crimes. Let’s have an brief review of the IT Act whether it is capable to control the cyber crimes in the country general and in banking industry in particular. Some of the strength and weaknesses of the act are as under:-

1) The IT Act 2000 empowers the government departments to accept filing, creating and retention of official documents in the digital format. The Act also puts forward the proposal for setting up the legal framework essential for the authentication and origin of electronic records / communications through digital signature.

2) The Act is silent over the e-mails and not approved in a court of law.
3) The act also talks about digital signatures and digital records. Digital signature and digital record can be produced as an evidence in the court of law and have been also awarded the status of being legal and valid means that can form strong basis for launching litigation in a court of law.

4) The Act now allows Government to issue notification on the web. This the beginning of e-governance in India.

5) It makes the task simple for the companies for filing any form, application or document by laying down the guidelines to be submitted at any appropriate office, authority, body or agency owned or controlled by the government.

6) The act also provides statutory remedy to the corporate in case the crime against the accused for breaking into their computer systems or network and damaging and copying the data is proven. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore ($200,000).

7) Also the law sets up the Territorial Jurisdiction of the Adjudicating Officers for cyber crimes and the Cyber Regulations Appellate Tribunal.

8) The law has also laid guidelines for providing Internet Services on a license on a non-exclusive basis.

A critical evolution is required to assess whether the cyber laws of the country are sufficient and secure enough to provide a strong platform to the country’s e-commerce business and e-banking. With the passage of time, as technology developed further and new methods of committing crime using Internet & computers surfaced, the need was felt to amend the IT Act, 2000 to insert new kinds of cyber offences and plug in other loopholes that posed hurdles in the effective enforcement of the IT Act, 2000. This led to the passage of the Information Technology (Amendment) Act, 2008 which was made effective from 27 October 2009. The IT (Amendment) Act, 2008 has brought marked changes in the IT Act, 2000 on several counts.

The Information Technology Act, 2000 and its amendment in 2008, though provides certain kind of protection, but does not cover all the spheres of the IT where protection must be provided. There is no enforcement machinery to ensure the protection of domain names on net.
3.3 CRITICAL EVALUATION OF INFORMATION TECHNOLOGY ACT 2000 AND AMENDMENT ACT 2008

3.3 CRITICAL EVALUATION OF ITACT2000 AND IT AMENDMENT ACT 2008

Information technology is basically related to the construction and gathering of information. It is also a phenomenon of processing, storage, presentation and dissemination of information. Information is a reservoir which has no importance until it is processed utilize and consumed. Information technology transacts with information system, data storage, access, retrieval, analysis and intelligent decision making. There is a penetrating effect of Information technology on individuals as well as on society. Information technology operates firmly on hardware and software of a computer and tele-communication infrastructure. But this is one side of the coin of the information Technology. The other aspects of the information technology are the challenges for the entire global society and at present it created the threat of cyber crimes and more over cyber terrorism. When Internet was first invented the founder of the Internet had no idea and they were never that internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulations. With the emergence of the technology the misuse of the technology has also expanded to its optimum level. The abuse of the information technology has created the need of the enactment of the cyber laws.

3.3.1 FOUNDATION BACKGROUND OF I.T. LESILATIONS IN INDIA

There is a well-defined legal system in India. Various legislations were enacted and leading among them is Constitution of India. The major legislation enacted were Indian Penal Code, the Indian Evidence Act 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934, the Companies Act, and other relevant Acts and Regulation to control and curb the crime. After the arrival of the internet and globally adoption of information technology, new types of problems of the law in this context started happening. None of the existing laws gave any legal validity or sanction to the
activities of internet in Cyberspace. To control these contemporary legal problems arose due to internet the necessity of enactment of new legislation felt in the country.

9th decade of the last century witnessed the momentum in globalization and computerisation. Maximum nations embraced the information technology and computerization in the various fields of operation. Due to advent of technology and expansion in use of internet there is a enormous growth in e-commerce. Prior to the implementation of information technology and use of internet most of the transactions of international trade and commerce were done through documents being transmitted through post and by telex only. In the same manner evidences and records were predominantly kept either in the form of paper or other forms of hard-copies only. Due to increased volume of international trade being conducted through electronic communication and its other form like email and gaining impetus, an urgent requirement was felt for reorganization of records in the form of electronic i.e. the data what is stored in a computer or an external storage devices attached thereto.

The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on e-commerce in 1996. The General Assembly of United Nations passed a resolution in January 1997 inter alia, recommending all States in the UN to give favorable considerations to the said Model Law, which provides for recognition to electronic records and according it the same treatment like a paper communication and record.

**Major reasons for enactment of I.T. legislations in India**

a) Domestic Reasons

1. Growing volume of business transactions with a extensive use of Information Technology and Internet.
2. Cost of transaction by use the technology is cheaper than the traditional method as it is easier, faster and cheaper to store, transact and communicate electronic information.
3. The business persons are fully conversant with the advantages of use of technology but at the same time they were hesitant to embrace the new method as there was no legal protection under the existing laws
2. External Reasons
Following are the external reasons mainly responsible for the enactment of the IT Act, 2000:

i. Many countries have accepted the Information technology and change the traditional method of business and accepted the e-commerce which is based on internet technology. Moreover there was many fold rise in the international trade and business and it is convenient to handle the business in volume.

ii. The then Department of Electronics (DoE) was given the mandate to have an enactment in place, on the lines of the UNCITRAL’s Model Law on Electronic Commerce soon after its adoption by the UN General Assembly. It was a foresight on the part of the Government of India to initiate the entire process of enacting India’s first ever information technology legislation soon after its adoption by the UN General Assembly

Under these situations Government of India enacted the Information Technology Act, 2000 based on the UNCITRAL’s Model Law on Electronic Commerce. It received the assent of the President on the June 9, 2000 and came into force on October 17, 2000.

3.3.2 AIMS AND OBJECTIVES OF INFORMATION TECHNOLOGY ACT, 2000

The preamble of the Information Technology Act, 2000 reads “An Act to provide legal recognition for transactions carried out by means of electronic communication, commonly referred to as “electronic commerce” which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies”.

As per the preamble of the Information Technology Act is formulated as
(a) A facilitating Act,
(b) An enabling Act, and
(c) A regulating Act

261 Sharma V., Part B- An Overview of cyber law, paper I, Introduction to the cyber world and cyber Law published on http://www.elearningilidelhi.org/eSikshak/other/Courses/Course101/Module9/OVERVIEW OF CYBER LAW
(a) A Facilitating Act
Being the facilitating the Information Technology Act, 2000 is a facilitating Act facilitates e-commerce and in turn e-banking. Besides the e-commerce and e-governance it also facilitates the e-governance though there is no mention of e-governance in the UNCITRAL Model Law of E-commerce. It is pertinent to note here that the Information Technology Act is based on the UNICITROL Model Law. This Act facilitates the e-governance and the entire ‘Chapter III’ of the Act is devoted to e-governance.

(b) An Enabling Act
Being the enabling act, the Information Technology Act, 2000 enables a legal regime of electronic records and digital signatures. The Act creates the legal binding to meet the fundamental requirement of all the electronic records, communications or transactions taken place on the internet.

(c) A Regulating Act
Being the regulating Act, the Information Technology Act, 2000 regulates cyber crimes against the individuals and government organisations like banks etc. This Act not only controls the cyber crime but also provides a remedial measures for infringements and offences.

It makes clear from the aims and objectives of the act that for the promotion of the e-commerce in India, Government had to suitably amend the existing laws in India. Electronic records and digital signature was to be brought under the preview of legal recognition. Data Interchange (EDI) and other means of electronic communication was to be brought under the preview of legal recognition. To business contacts and creation of rights and obligations through electronic media was to be brought under the preview of legal recognition. To create a governing body to supervise the certifying authorities issuing digital signature certificates. To prevent misuse of the e-business transactions and also to established civil and criminal liabilities for infringement of the provisions of the Act and to encourage the use and acceptance of electronic records and digital signatures in government offices and agencies and also to facilitate e-governance. This was the effort initiated by the government to make the citizen-government interaction more hassle free. Similarly to make major amendments in the Indian Penal Code, 1860
and the Indian Evidence Act, 1872 to provide for corresponding changes in the various provisions which deal with offences relating to documents and paper based transactions. To facilitate electronic fund transfers between the financial institutions. Reserve Bank of India Act, 1934 was to be suitably amended. To suitably amend the Banker’s Books Evidence Act, 1891 to provide the legal sanctity for books of accounts maintained in the electronic form by the banks. To make the domestic laws in fine tune with Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) adopted by the General Assembly of the United Nations. Whatever stated in the foregoing paragraphs it reveals that the Information Technology Act2000 fundamentally deals with the following issues:

1. Legal Recognition of Electronic Documents
2. Legal Recognition of Digital Signatures
3. Offenses and Contraventions
4. Justice Dispensation Systems for cyber crimes

3.3.3 OVERVIEW OF THE INFORMATION TECHNOLOGY ACT, 2000262

The Information Technology Act was enacted with a view to give a fillip to the growth of electronic based transactions, to provide legal recognition for ecommerce and e-transactions, to facilitate e-governance, to prevent computer based crimes and ensure security practices and procedures in the context of widest possible use of information technology worldwide

Applicability of the Act

The Act will apply to the whole of India unless otherwise mentioned. It applies also to any offence or contravention there under committed outside India by any person.

The Act shall not apply to the following documents or transactions –

> A negotiable instrument as defined in Sec.13 of the Negotiable Instruments Act, 1881;
> A power of attorney as defined in Sec.1A of the Powers of Attorney Act, 1882;
> A trust as defined in Section 3 of the Indian Trusts Act, 1882;

262 Adukia and associates chartered accountant, article overview of cyber crimes in India
A Will as defined in Sec.2(h) of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called;

Any contract for the sale or conveyance of immovable property or any interest in such property.

3.3.4 STRUCTURE OF THE INFORMATION TECHNOLOGY ACT 2000

- Chapter – I – Preliminary
- Chapter – II – Digital Signature and Electronic Signature (Sections 3 & 3A)
- Chapter – III – Electronic Governance (Sections 4 to 10A)
- Chapter – IV – Attribution, Acknowledgement and Dispatch of Electronic Records (Sections 11 to 13)
- Chapter – V – Secure electronic records and secure electronic signatures (Sections 14 to 16)
- Chapter – VI – Regulation of Certifying Authorities (Sections 17 to 34)
- Chapter – VII – Electronic Signature Certificates (Sections 35 to 39)
- Chapter – VIII – Duties of Subscribers (Sections 40 to 42)
- Chapter – IX – Penalties, Compensation and Adjudication (Sections 43 to 47)
- Chapter X – The Cyber Appellate Tribunal (Sections 48 to 64)
- Chapter XI – Offences (Sections 65 to 78)
- Chapter XII – Intermediaries not to be liable in certain cases (Section 79)
- Chapter XII – Network service providers not to be liable in certain cases (Section 79)
- Chapter XIII – Miscellaneous (Sections 80 to 90)
- First Schedule – Amendments to the Indian penal code, 1860 (45 of 1860) (Section 91)
- Second Schedule – Amendments to the Indian Evidence Act, 1872 (1 of 1872) (Section 92)
- Third Schedule – Amendments to the Bankers’ Books Evidence Act, 1891 (18 of 1891) (Section 93)
- Fourth Schedule – Amendment to the Reserve Bank of India act, 1934 (2 of 1934) (Section 94)

263 Information Technology Act, 2000
3.3.4(A).CHAPTER-I

SECTION-1 -SHORT TITLE, EXTENT, COMMENCEMENT AND APPLICATION

Shot Title of the Act:-This Act may be called the Information Technology Act, 2000.

Extent of the Act: - It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention there under committed outside India by any person.

Commencement of the Act:- It shall come into force on such date as the Central Government may, by notification, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision.

Application of the Act: - Nothing in this Act shall apply to,

(a) A negotiable instrument as defined in section 13 of the Negotiable Instruments Act,1881.

(b) A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882.

(c) A trust as defined in section 3 of the Indian Trusts Act, 1882.

(d) A will as defined in clause (h) of section 2 of the Indian Succession Act,1925 including any other testamentary disposition by whatever name called.

(e) Any contract for the sale or conveyance of immovable property or any interest in such property;

(f) Any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

IMPORTANT DEFINITIONS OF THE TERMS RELATED TO CYBER LAW

Section 2 of Information Technology Act defines the various important terms as under:-

"Access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network. (Sec.2 (1) (a) of IT Act, 2000)
"Addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary. (Sec.2 (1)(b) of IT Act, 2000)

"Affixing Digital Signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Electronic Signature. (Sec.2 (1) (d) of IT Act, 2000)

"Asymmetric Crypto System" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature. (Sec. 2(1) (f) of IT Act, 2000)

"Certifying Authority" means a person who has been granted a license to issue a Electronic Signature Certificate under section 24. (Sec.2(1)(g) of IT Act, 2000)

"Computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network (Sec.2 (1) (i) of IT Act, 2000)

"Computer Network" means the interconnection of one or more Computers or Computer systems or Communication device through-
(i) The use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and
(ii) Terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained. (Sec.2 (1) (j) of IT Act, 2000)

"Computer Resource" means computer, communication device, computer system, computer network, data, computer database or software. (Sec. 2(1) (k) of IT Act, 2000)

"Computer System" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data, and output data, that performs logic, arithmetic, data
storage and retrieval, communication control and other functions. (Sec.2 (1) (l) of IT Act, 2000)

"Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer. (Sec.2 (1) (o) of IT Act, 2000)

"Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3. (Sec.2 (1) (p) of IT Act, 2000)

"Electronic Form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device. (Sec.2 (1) (r) of IT Act, 2000)

"Electronic Record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche. (Sec.2 (1) (t) of IT Act, 2000)

"Function", in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer. (Sec.2 (1) (u) of IT Act, 2000) "Information" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche. (Sec.2 (1) (v) of IT Act, 2000)

"Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes. (Sec.2 (1) (w) of IT Act, 2000)

"Key Pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key. (Sec.2 (1) (x) of IT Act, 2000)
"Originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary. (Sec.2 (1) (za) of IT Act, 2000)

"Private Key" means the key of a key pair used to create a digital signature. (Sec.2 (1) (zc) of IT Act, 2000)

"Public Key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate. (Sec.2 (1) (zd) of IT Act, 2000)

3.3.4(B).CHAPTER II

IMPORTANT PROVISIONS OF THE IT ACT2000

1) DIGITAL SIGNATURE264

Section 3 of IT Act dealt with the ‘Digital Signature’. The section deals with the conditions subject to which an electronic record may be authenticated by means of affixing digital signature to provide authenticity, integrity, secrecy and non-repudiation to electronic record or message. It also uses the internet as a safe and secure medium without any violation of e-transaction on the internet.

IT Act, 2000 provides the legal provision relating to digital signature as under:

- Authentication of electronic records
- Authentication by use of asymmetric crypto system and hash function
- Verification of electronic record.
- Private key and public key are unique to the subscriber and constitute a functioning key pair

Therefore ‘Digital Signature’ is a means to ensure validity of electronic transactions in the cyber space.

3.3.4(C).CHAPTER-III

2) E-GOVERNANCE

Sections 4 to10A of the IT Act, 2000 dealt with E-governance or Electronic Governance.

264 Section 3 of ITAct2000
Legal recognition of Electronic Records

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then despite of whatever thing contained in such law, such requirement shall be deemed to be satisfied if such information or matter is rendered or made available in an electronic form and accessible so as to be usable for a subsequent reference (Sec.4)

Legal recognition of Digital Signature

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then despite of whatever thing contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government. For the purposes of this section, "signed", is used with reference to a person it mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be interpreted accordingly. (Sec.5)

Use of electronic records and digital signatures in Government and its agencies

Where any law provides for

i) The filing of any application form or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner

ii) The issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner

iii) The receipt or payment of money in a particular manner, then despite of whatever thing contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

The appropriate Government may, by rules, prescribe

---

265 Sec 4 of IT Act 2000
266 Sec 5 of IT Act 2000
267 Sec 6 of IT Act 2000
i) The manner and format in which such electronic records shall be filed, created or issued or
ii) The manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (i).

**Retention of electronic records**

Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if:

i) The information contained therein remains accessible so as to be usable for a subsequent reference

ii) The electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received.

iii) The details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record: Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records (Sec.7)

**Publication of rule, regulation, etc., in Electronic Gazette**

Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette. Provided that where any rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.(Sec.8)

---

268 Sec.7 of ITAct2000
269 Sec.8 of ITAct2000
Sections 6, 7 and 8 not to confer right to insist document should be accepted in electronic form\(^{270}\)

Nothing contained in sections 6, 7 & 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.(Sec.9)

**Power to make rules by Central Government in respect of digital signature\(^{271}\)**

The Central Government may, for the purposes of this Act, by rules, prescribe:-

i) The type of digital signature;

ii) The manner and format in which the digital signature shall be affixed;

iii) The manner or procedure which facilitates identification of the person affixing the digital signature;

iv) Control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

v) Any other matter which is necessary to give legal effect to digital signatures(Sec10)

**The following are some of the applications of E-Governance**

- MCA21 – a Mission Mode project under NEGP (National e-governance plan) which is one of the first few e-Governance projects under NEGP to successfully implement Digital Signatures in their project.
- Income Tax e-filing
- Indian Railway Catering and Tourism Corporation (IRCTC)
- Director General of Foreign Trade (DGFT)
- RBI Applications (SFMS : structured Financial Messaging System)
- National e-Governance Services Delivery Gateway (NSDG)
- E-Procurement
- E-Office
- E-District applications of UP, Assam etc

\(^{270}\) Sec.9 of ITAct2000  
\(^{271}\) Sec.10 of ITAct2000
Gyandoot Project (Madhya Pradesh)
Gramdoot (Rajasthan)
Bhoomi (Karnataka)
Warana (Maharashtra)
Single Window Clearance System (Delhi)

3.3.4(D). CHAPTER-IV

3) ATTRIBUTION, ACKNOWLEDGEMENT AND DISPATCH OF ELECTRONIC RECORDS

ATTRIBUTION OF ELECTRONIC RECORDS

Sec.11 of the IT Act, 2000 dealt with Attribution of electronic records. An electronic record will be attributed to the originator - if it was sent by the originator himself; or by a person who had the authority to act on behalf of the originator in respect of that electronic record; or by an information system programmed by or on behalf of the originator to operate automatically.

Acknowledgment of receipt

Section 12 of the IT Act communicates that where the originator has not agreed with the addressee that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by any communication by the addressee, automated or otherwise, or any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

The section also implies that where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.

Similarly, the section also speak that where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or

---

272 Sec.11 of ITAct2000
273 Sec.12 of ITAct2000
agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

**Time and place of dispatch and receipt of electronic record**

Time and place of dispatch and receipt of electronic record is covered under Sec.13 of the IT Act, 2000. Electronic record enters a computer resource outside the control of the originator the dispatch of an electronic record occurs. The time of receipt of an electronic record will be determined unless agreed between the originator and the addressee,

a) If the addressee has designated a computer resource for the purpose of receiving electronic records when receipt occurs at the time when the electronic record enters the designated computer resource; or if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

An electronic record is generally deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business. If the originator or the addressee has more than one place of business, the principal place of business will be the place of business. If the originator or the addressee does not have a place of business, his usual place of residence will be deemed to be the place of business. "Usual Place of Residence", in relation to a body corporate, means the place where it is registered.

---

274 Sec.13 of ITAct2000
3.3.4(E).CHAPTER-V

4) SECURE ELECTRONIC RECORDS AND SECURE DIGITAL SIGNATURES

Secure electronic record\textsuperscript{275}
Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be secure electronic record from such point of time to the time of verification.(Sec.14)

Secure electronic signature \textsuperscript{276}
An electronic signature shall be deemed to be secure electronic signature if by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was unique to the subscriber affixing it: capable of identifying such subscriber and created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated, then such digital signature shall be deemed to be a secure digital signature(Sec.15)

Security Procedure\textsuperscript{277}
The Central Government shall for the purposes of this Act prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including the nature of the transaction; the level of sophistication of the parties with reference to their technological capacity; the volume of similar transactions engaged in by other parties; the availability of alternatives offered to but rejected by any party; the cost of alternative procedures; and the procedures in general use for similar types of transactions or communications

\textsuperscript{275} Sec.14 of IT Act2000
\textsuperscript{276} Sec.15 of IT Act2000
\textsuperscript{277} Sec.16 of ITAct2000
5) REGULATION OF CERTIFYING AUTHORITIES

A Certifying Authority is a trusted body, whose central responsibility is to issue, revoke, renew and provide directories of Digital Certificates. Certifying Authority means a person who has been granted a license to issue an Electronic Signature Certificate under section 24. Provisions with regard to Certifying Authorities are covered under Chapter VI i.e. Sec.17 to Sec.34 of the IT Act, 2000. It contains detailed provisions relating to the appointment and powers of the Controller and Certifying Authorities.

Appointment of Controller and other officers

Sec.17(1) of ITAct 2000 implies that the Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers and Assistant Controllers as it deems fit.

Sec.17 (2) of IT Act 2000 implies that The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.

Sec.17 (3) of IT Act 2000 implies that the Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

Sec.17(4) of IT Act 2000 implies that The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Central Government.

Sec17(5) of ITAct2000 implies that The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

Sec17 (6) of ITAct2000 implies that there shall be a seal of the Office of the Controller

Following are the functions of controller namely:

(a) To exercise supervision over the activities of the Certifying Authorities.

---

278 Sec.17 of IT Act2000
279 Sec.18 of ITAct2000
(b) To certify public keys of the Certifying Authorities.
(c) To lay down the standards to be maintained by the Certifying Authorities.
(d) To specify the qualifications and experience which employees of the Certifying Authorities should possess.
(e) To specify the conditions subject to which the Certifying Authorities shall conduct their business.
(f) To specify the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key.
(g) To specify the form and content of a Digital Signature Certificate and the key.
(h) To specify the form and manner in which accounts shall be maintained by the Certifying Authorities.
(i) To specify the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them.
(j) To facilitate the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems.
(k) To specify the manner in which the Certifying Authorities shall conduct their dealings with the subscribers.
(l) To resolve any conflict of interests between the Certifying Authorities and the subscribers.
(m) To lay down the duties of the Certifying Authorities.
(n) To maintain a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

Recognition of foreign Certifying Authorities

Sec19(1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognize any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

---

Sec.19 of ITAct2000
Sec19(2) Where any Certifying Authority is recognised under sub-section (1), the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

Sec19(3) The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

**Controller to act as repository**

Section 20(1) of ITAct 2000 implies that the Controller shall be the repository of all Digital Signature Certificates issued under this Act.

Section 20(2) of ITAct 2000 implies that the Controller shall make use of hardware, software and procedures that are secure i.e., intrusion and misuse, observe such other standards as may be prescribed by the Central Government to ensure that the secrecy and security of the digital signatures are assured.

Section (3) of ITAct 2000 implies that the Controller shall maintain a computerised data base of all public keys in such a manner that such data base and the public keys are available to any member of the public.

**License to issue Digital Signature Certificates**

Section 21(1) of ITAct 2000 implies that subject to the provisions of sub-section (2), any person may make an application, to the Controller, for a license to issue Digital Signature Certificates.

Section(2) of ITAct 2000 implies that no license shall be issued under sub-section (1), unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue Digital Signature Certificates as may be prescribed by the Central Government.

Section(3) of ITAct 2000 implies that A license granted under this section shall be valid for such period as may be prescribed by the Central Government, not be transferable or heritable and be subject to such terms and conditions as may be specified by the regulations.

281 Sec. 20 of ITAct 2000
282 Sec. 21 of ITAct 2000
Application for license

Every application for issue of a license shall be in such form as may be prescribed by the Central Government. Every application for issue of a license shall be accompanied by a certification practice statement; a statement including the procedures with respect to identification of the applicant. Payment of such fees, not exceeding Rs.25, 000/- as may be prescribed by the Central Government and such other documents, as may be prescribed by the Central Government

Renewal of license

An application for renewal of a license shall be in such a form accompanied by such fees, not exceeding Rs.5000/, as may be prescribed by the Central Government and shall be made not less than 45 days before the date of expiry of the period of validity of the license

Procedure for grant or rejection of license

After receipt of application and after considering the documents attached with the application and other factors, the controller may grant the licence or reject the application. On the other hand before rejecting the application, the applicant should be given an opportunity of being heard

Suspension of license

The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has made a statement in, or in relation to, the application for the issue or renewal of the license, which is incorrect or false in material particulars, failed to comply with the terms and conditions subject to which the license was granted, failed to maintain the standards section 20, contravened any provisions of this Act, rule, regulation or order made there under, evoke the license: provided that no license shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation. The Controller may, if he has reasonable cause to believe that there is any ground for revoking a license by order

283 Sec.22 of ITAct2000
284 Sec.23 of IT Act2000
285 Sec.24 of ITAct2000
286 Sec.25 of ITAct 2000
suspend such license pending the completion of any inquiry ordered by him provided that no license shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension. No Certifying Authority whose license has been suspended shall issue any Digital Signature Certificate during such suspension.

Notice of suspension or revocation of license

As per the provisions of section 26 of ITAct 2000, the controller shall publish the notice of suspension or revocation of license of the Certifying Authority when suspended or revoked. Likewise where one or more repositories are specified, the Controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories:

Power to delegate

The Controller may, in writing, authorize the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this Chapter.

Power to investigate contraventions

Section 27(1) of ITAct 2000 implies that the Controller or any officer authorized by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made there under.

Section 27(2) of ITAct 2000 implies that the Controller or any officer authorized by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 and shall exercise such powers, subject to such limitations laid down under that

Access to computers and data

Section 29(1) of ITAct 2000 implies that without prejudice to the provisions of subsection (1) of section 69, the Controller or any person authorized by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this Act, rules or regulations made there under has been committed, have access to any

---

287 Sec.26 of ITAct2000
288 Sec.27 of ITAct2000
289 Sec.28 of ITAct2000
290 Sec.29 of ITAct2000
computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.(2) For the purposes of sub-section (1), the Controller or any person authorized by him may, by order, direct any person in-charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

**Certifying Authority to follow certain procedures**

Every Certifying Authority shall, make use of hardware, software and procedures that are secure from intrusion and misuse; provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions, adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured and observe such other standards as may be specified by regulations.

**Certifying Authority to ensure compliance of the Act, etc**

Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations and orders made there under.

**Display of license**

Every Certifying Authority shall display its license at a conspicuous place of the premises in which it carries on its business.

**33. Surrender of license**

Section 33(1) of ITAct 2000 implies that very Certifying Authority whose license is suspended or revoked shall immediately after such suspension or revocation, surrender the license to the Controller.

Section 33(2) of ITAct 2000 implies that where any Certifying Authority fails to surrender a license under sub-section (1), the person in whose favour a license is issued, shall be guilty of an offence and shall be punished with imprisonment which may extend up to six months or a fine which may extend up to ten thousand rupees or with both.

---

291 Sec.30 of ITAct2000
292 Sec.31 of ITAct2000
293 Sec.32 of ITAct2000
294 Sec.33 of ITAct2000
Disclosure

Section 34(1) of ITAct 2000 implies that every Certifying Authority shall disclose in the manner specified by regulations; its Digital Signature Certificate which contains the public key corresponding to the private key used by the Certifying Authority to digitally sign another Digital Signature Certificate; any certification practice statement relevant thereto; notice of the revocation or suspension of its Certifying Authority certificate, if any and any other fact that materially and adversely affects either the reliability of a Digital Signature Certificate, which that Authority has issued, or the Authority’s ability to perform its services.

Section 34(2) of ITAct 2000 implies that where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Digital Signature Certificate was granted, then, the Certifying Authority shall use reasonable efforts to notify any person who is likely to be affected by that occurrence or act in accordance with the procedure.

3.3.4(G). CHAPTER-VII

6) DIGITAL SIGNATURE CERTIFICATES

Certifying Authority to issue Digital Signature Certificate

Any person can make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Central Government.

Every such application shall be accompanied by such fee not exceeding Rs. 25,000/- as may be prescribed by the Central Government, to be paid to the Certifying Authority.

Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

Sec. 34 of ITAct 2000
Sec. 35 of ITAct 2000
On receipt of an application the Certifying Authority may, after consideration of the certification practice statement and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application:

Provided that no Digital Signature Certificate shall be granted unless the Certifying Authority is satisfied that The applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate. The applicant holds a private key, which is capable of creating a digital signature. The public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant.

**Representations upon issuance of Digital Signature Certificate**\(^{297}\)

A Certifying Authority while issuing a Digital Signature Certificate shall certify that—

(a) It has complied with the provisions of this Act and the rules and regulations made there under,

(b) It has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it.

(c) The subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate.

(d) The subscriber’s public key and private key constitute a functioning key pair.

(e) The information contained in the Digital Signature Certificate is accurate.

(f) It has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations made in clauses (a) to (d).

**Suspension of Digital Signature Certificate**\(^{298}\)

Subject to the provisions of sub-section (2), the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate on receipt of a request to that effect from the subscriber listed in the Digital Signature Certificate or

\(^{297}\) Sec.36 of ITAct2000

\(^{298}\) Sec.37 of ITAct2000
any person duly authorized to act on behalf of that subscriber if it is of opinion that the
Digital Signature Certificate should be suspended in public interest
A Digital Signature Certificate shall not be suspended for a period exceeding 15 days
unless the subscriber has been given an opportunity of being heard in the matter.
On suspension of a Digital Signature Certificate under this section, the Certifying
Authority shall communicate the same to the subscriber

**Revocation of Digital Signature Certificate**

A Certifying Authority may revoke a Digital Signature Certificate issued by it where the
subscriber or any other person authorized by him makes a request to that effect or upon
the death of the subscriber, or upon the dissolution of the firm or winding up of the
company where the subscriber is a firm or a company. Subject to the provisions of sub-
section and without prejudice to the provisions of sub-section (1),
Certifying Authority may revoke a Digital Signature Certificate which has been issued by
it at any time, if it is of opinion that a material fact represented in the Digital Signature
Certificate is false or has been concealed; a requirement for issuance of the Digital
Signature Certificate was not satisfied. A Digital Signature Certificate shall not be
revoked unless the subscriber has been given an opportunity of being heard in the
matter. On revocation of a Digital Signature Certificate under this section, the Certifying
Authority shall communicate the same to the subscriber.

**Notice of suspension or revocation**

Section 39(1) of ITAct 2000 implies that where a Digital Signature Certificate is
suspended or revoked under section 37 or section 38, the Certifying Authority shall
publish a notice of such suspension or revocation, as the case may be, in the repository
specified in the Digital Signature Certificate for publication of such notice.
Section 39(2) of ITAct 2000 implies that where one or more repositories are specified,
the Certifying Authority shall publish notices of such suspension or revocation, as the
case may be in all such repositories

---

299 Sec.38 of ITAct 2000
300 Sec.39 of ITAct 2000
7) DUTIES OF SUBSCRIBERS

Meaning of Subscriber

Electronic Signature Certificate issued is termed as “Subscriber”

Generating key pair

The subscriber shall generate the key pair by applying the security procedure on the publication of a Digital Signature Certificate the subscriber shall be deemed to have accepted a Digital Signature Certificate

a) To one or more persons,

b) In a repository, or

c) otherwise demonstrates his approval of the Digital Signature

By accepting a Digital Signature Certificate the subscriber certifies that:

a) The subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same.

b) All representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true.

c) All information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

Control of private key

Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to any other person

If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by .the regulations.

The liability of the subscriber shall be hold till the information to the Certifying Authority has not been given by him that the private key has been compromised.
3.3.4(I).CHAPTER-IX

8) PENALTIES AND ADJUDICATION

Penalty for damage to computer, computer system, etc

If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network shall be held liable to pay damages by way of compensation to the person so affected in the following :-

a. If a person tried to accesses or secures access to such computer, computer system or computer network;

b. If a person downloads copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium.

c. If a person Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network.

d. If a person damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network.

e. If a person disrupts or causes disruption of any computer, computer system or computer network.

f. If a person denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means.

g. If a person provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under.

h. If a person charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Following terms are explained for the purposes of this section as under:-

304 Sec.43 of ITAct 2000
"Computer contaminant" means any set of computer instructions that are designed to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or by any means to usurp the normal operation of the computer, computer system, or computer network;

"Computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network.

"Computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme or instruction is executed or some other event takes place in that computer resource.

"Damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

**Penalty for failure to furnish information return, etc**

If any person who is required under this Act or any rules or regulations fails to comply with the following will be held responsible as under

a. If any person fails to furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure.

b. If any person fails to file any return or furnish any information, books or other documents within the time specified therefore in the regulations fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues.

c. If any person fails to maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

---

305 Sec.44 of IT Act 2000
Residuary penalty\textsuperscript{306}

Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding Rs.25,000/- to the person affected by such contravention or a penalty not exceeding Rs.25,000/-. 

Power to adjudicate\textsuperscript{307}

If any person who has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made there the Central Government shall appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government. The adjudicating officer shall, after giving the person a reasonable opportunity for making representation in the matter and if he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section. Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under sub-section (2) of section 58, and 

(a) All proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code. 

(b) Shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973. 

Factors to be taken into account by the adjudicating officer\textsuperscript{308}. 

While adjudging the quantum of compensation under this section, the adjudicating officer shall have to consider the following factors, as under:-

d) The amount of gain of unfair advantage, wherever quantifiable, made as a result of the default. 

e) The amount of loss caused to any person as a result of the default. 

f) The repetitive nature of the default

\textsuperscript{306} Sec.45 of ITAct2000 
\textsuperscript{307} Sec.46 of ITAct2000 
\textsuperscript{308} Sec.47 of ITAct 2000
3.3.4(J)CHAPTER-X

9) THE CYBER REGULATIONS APPELLATE TRIBUNAL

Establishment of Cyber Appellate Tribunal

1) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Regulations Appellate Tribunal

2) The Central Government shall specify, the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

Composition of Cyber Appellate Tribunal

Section 49 of IT Act 2000 implies that a Cyber Appellate Tribunal shall be consisted of one person only (hereinafter referred to as the Residing Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government.

Qualifications for appointment as Presiding Officer of the Cyber Appellate Tribunal

Section 50 of ITAct implies that a person shall not be qualified for appointment as the Presiding Officer of a Cyber Appellate Tribunal unless he is, or has been. or is qualified to be, a Judge of a High Court, or is or has been a member of the Indian Legal Service and is holding or has held a post in Grade 1 of that Service for at least three years.

Term of office

Section 51 of the ITAct2000 implies that the Presiding Officer of a Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of 65 years, whichever is earlier.
Salary, allowances and other terms and conditions of service of Presiding Officer \(^{313}\)

As prescribed by the section 52, the salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of the Presiding Officer of a Cyber Appellate Tribunal, provided that neither the salary and allowances nor the other terms and conditions of service of the Presiding Officer shall be varied to his disadvantage after appointment.

Filling up of vacancies \(^{314}\)

Section 53 of ITAct 2000 implies that due to the reason other than temporary absence, any vacancy occurs in the office and the Presiding Officer of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

Resignation and removal \(^{315}\)

Provisions of the section 54(1) implies that the Presiding Officer of a Cyber Appellate Tribunal may, by notice in writing resign his office provided that

- unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or
- until a person duly appointed as his successor enters upon his office or
- until the expiry of his term of office, whichever is the earliest.

Provisions of the section 54(2) provides that the Presiding Officer of a Cyber Appellate Tribunal shall not be removed from his office except by an order by the Central Government on the ground of proved misbehavior or incapacity after an inquiry made by a Judge of the Supreme Court in which the Presiding Officer concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.

\(^{313}\) Sec.52 of ITAct 2000
\(^{314}\) Sec.53 of IT Act 2000
\(^{315}\) Sec.54 of IT Act 2000
Provisions of Section 54(3) provide that the Central Government may, by rules, regulate the procedure for the investigation of misbehavior or incapacity of the aforesaid Presiding Officer.

Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings\(^{316}\)

The provisions of the section 55 of ITAct2000 are such that merely on the ground of any defect in the constitution of a Cyber Appellate Tribunal, no order of the Central Government appointing any person as the Presiding Officer of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question.

Staff of the Cyber Appellate Tribunal\(^{317}\)

Section 56(1) of the IT Act 2000 implies that the Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as that Government may think fit.

Section 56(2) of the IT Act 2000 implies that the officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Presiding Officer.

Section 56(3) of the IT Act 2000 implies that the salaries, allowances and other conditions of service of the officers and employees or the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

Appeal to Cyber Appellate Tribunal\(^{318}\)

Section 57(1) of IT Act 2000 implies that as provided in sub-section (2), any person aggrieved by an order made by Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter.

Section 57(2) of IT Act 2000 implies that no appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.

Section 57(3) implies that every appeal under sub-section (1) shall be filed within a period of twenty-five days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved and it shall be

---

\(^{316}\) Sec.55 of IT Act2000

\(^{317}\) Sec.56 of ITAct 2000

\(^{318}\) Sec.57 of ITAct 2000
in such form and be accompanied by such fee as may be prescribed subject to the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of 25 days if it is satisfied that there was sufficient cause for not filing it within that period. Section 57(4) of the IT Act 2000 implies that on receipt of an appeal under sub-sec. (1), the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against. Section 57(5) of the IT Act 2000 implies that the Cyber Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned Controller or adjudicating officer. Section 57(6) of the IT Act 2000 implies that the appeal filed before the Cyber Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavor shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

**Procedure and powers of the Cyber Appellate Tribunal**

**Procedure of the CAT:**-Section 58(1) of the ITAct 2000 implies that the Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

**Power of the CAT:**-Section 58(2) of the ITAct 2000 implies that the Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters:-

(a) Summoning and enforcing the attendance of any person and examining him on oath.
(b) Requiring the discovery and production of documents or other electronic records.
(c) Receiving evidence on affidavits.
(d) Issuing commissions for the examination of witnesses or documents.
(e) Reviewing its decisions.

319 Sec.58 of ITAct 2000
(f) Dismissing an application for default or deciding it ex pane.
(g) Any other matter which may be prescribed.

**Proceedings of the Cyber Appellate Tribunal:** Section 58 (3) of the IT Act 2000 implies that every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

**Right to legal representation**
As per the legal provisions of section 59 of the IT Act 2000, the appellant may either appear in person or authorize one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal.

**Limitation**
As per the provisions of section 60 of the IT Act 2000, the provisions of the Limitation Act, 1963, shall, as far as may be, apply to an appeal made to the Cyber Appellate Tribunal.

**Civil court not to have jurisdiction**
As per the legal provisions of section 61 of the IT Act 2000, no court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

**Appeal to High Court**
As per the provisions of the section 62 of the IT Act 2000, any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order.

---

320 Sec.59 of IT Act 2000
321 Sec.60 of IT Act 2000
322 Sec.61 of IT Act 2000
323 Sec.62 of IT Act 2000
Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

**Compounding of contraventions**
Section 63(1) of the IT Act 2000, any contravention under this Chapter may, either before or after the institution of adjudication proceedings, be compounded by the Controller or such other officer as may be specially authorized by him in this behalf or by the adjudicating officer, as the case may be, subject to such conditions as the Controller or such other officer or the adjudicating officer may specify. Provided that such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded.

Section 63(2) of IT Act 2000, nothing in sub-section (1) shall apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded subject to any second or subsequent contravention committed after the expiry of a period of three years from the date on which the contravention was previously compounded shall be deemed to be a first contravention.

Section 63(3) of IT Act 2000, where any contravention has been compounded under sub-section (1), no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

**Recovery of penalty**
A penalty imposed under section 64 of the IT Act 2000, if it is not paid, shall be recovered as an arrear of land revenue and the license or the Digital Signature Certificate, as the case may be, shall be suspended till the penalty is paid.

---

324 Sec.63 of IT Act 2000  
325 Sec.64 of IT Act 2000
3.3.4(K).CHAPTER-XI

10) OFFENSES

Tampering with computer source documents\textsuperscript{326}

Any person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both. For this section "\textit{Computer source code}" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Hacking with computer system\textsuperscript{327}

Section 66(1) of ITAct 2000 implies that any person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.

Section 66(2) of ITAct 2000 implies that any person commits hacking shall be punished with imprisonment up to 3 years, or with fine which may extend up to Rs.2,00,000/-, or with both.

Publishing of information which is obscene in electronic form\textsuperscript{328}

Any person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to 5 years and with fine which may extend to Rs.1,00,000/-and in the event of a

\textsuperscript{326} Sec.65 of IT Act 2000
\textsuperscript{327} Sec.66 of IT Act 2000
\textsuperscript{328} Sec.67 of IT Act 2000
second or subsequent conviction with imprisonment of either description for a term which may extend to 10 years and also with fine which may extend to Rs.2,00,000/-.  

**Power of Controller to give directions**

Section 68(1) of ITAct 2000 implies that the Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.

Section 68(2) of ITAct 2000 implies that any person who fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding three years or to a Fine not exceeding two lakh rupees or to both.

**Directions of Controller to a subscriber to extend facilities to decrypt information**

Section 69(1) of ITAct 2000 implies that if the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

Section 69(2) of ITAct 2000 implies that the subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information.

Section 69(3) of ITAct 2000 implies that the subscriber or any person who fails to assist the agency referred to in sub-section (2) shall be punished with an imprisonment for a term which may extend to 7 years.

---

329 Sec.68 of IT Act 2000
330 Sec.69 of IT Act 2000
**Protected system**

Section 70(1) of ITAct 2000 implies that the appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.

Section 70(2) of ITAct 2000 implies that the appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1).

Section 70(3) of ITAct 2000 implies that any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to 10 years and shall also be liable to fine.

**Penalty for misrepresentation**

Any person makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be. He shall be punished with imprisonment for a term which may extend to 2 years, or with fine which may extend to Rs.1,00,000/-, or with both.

**Penalty for breach of confidentiality and privacy**

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to 2 years, or with fine which may extend to Rs.1,00,000/-, or with both.

---

331 Sec.70 of IT Act 2000  
332 Sec.71 of IT Act 2000  
333 Sec.72 of IT Act 2000
Penalty for publishing Digital Signature Certificate false in certain particulars  
Section 73(1) of ITAct 2000 implies that no person shall publish a Digital Signature 
Certificate or otherwise make it available to any other person with the knowledge that:- 
(a) The Certifying Authority listed in the certificate has not issued it; or 
(b) The subscriber listed in the certificate has not accepted it; or 
(c) The certificate has been revoked or suspended, unless such publication is for the 
purpose of verifying a digital signature created prior to such suspension or revocation. 
Section 73(2) of ITAct 2000 implies that any person who contravenes the provisions of 
sub-section (1) shall be punished with imprisonment for a term which may extend to two 
years, or with fine which may extend to Rs. 1,00,000/-, or with both.  
Publication for fraudulent purpose 
Any person knowingly creates, publishes or otherwise makes available a Digital 
Signature Certificate for any fraudulent or unlawful purpose shall be punished with 
imprisonment for a term which may extend to 2 years, or with fine which may extend to 
Rs. 1,00,000/-, or with both.  
Act to apply for offence or contravention committed outside India  
Section 75(1) of ITAct 2000 implies that subject to the provisions of sub-section (2), the 
provisions of this Act shall apply also to any offence or contravention committed 
outside India by any person irrespective of his nationality. 
Section 75(2) of ITAct 2000 implies that for the purposes of sub-section (1), this Act shall 
apply to an offence or contravention committed outside India by any person if the act or 
conduct constituting the offence or contravention involves a computer, computer system 
or computer network located in India.  
Confiscation 
Any computer, computer system, floppies, compact disks, tape drives or any other 
accessories related thereto, in respect of which any provision of this Act. rules, orders or

---

334 Sec.73 of IT Act 2000  
335 Sec.74 of IT Act 2000  
336 Sec.75 of IT Act 2000  
337 Sec.76 of IT Act 2000
regulations made there under has been or is being contravened, shall be liable to confiscation.

Nevertheless where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit.

Penalties or confiscation not to interfere with other punishments

No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

Power to investigate offences

Despite of whatever contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this Act.

3.3.4(L).CHAPTER-XII

11) NETWORK SERVICE PROVIDERS NOT TO BE LIABLE IN CERTAIN CASES

Network service providers not to be liable in certain cases

No person providing any service as a network service provider shall be liable under section 79 of IT Act 2000, rules or regulations made there under for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention where "Network service

338 Sec.77 of IT Act 2000
339 Sec.78 of IT Act 2000
340 Sec.79 of ITAct 2000
"provider" means an intermediary. "Third party information" means any information dealt with by a network service provider in his capacity as an intermediary.

3.3.4(M). CHAPTER-XIII

12) NETWORK SERVICE PROVIDERS NOT TO BE LIABLE IN CERTAIN CASES

Power of police officer and other officers to enter, search, etc.341
Section 80(1) of ITAct 2000 implies that despite of whatever contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected or having committed or of committing or of being about to commit any offence under this Act where "public place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

Section 80(2) of ITAct 2000 implies that where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

Section 80(3) of ITAct 2000 implies that the provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

Act to have overriding effect342

The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

Controller, Deputy Controller and Assistant Controllers to be public servants343

The Presiding Officer and other officers and employees of a Cyber Appellate Tribunal, the Controller, the Deputy Controller and the Assistant Controllers shall be deemed to be public servants within the meaning of section 21 of the Indian Penal Code.

341 Sec.80 of ITAct 2000
342 Sec.81 of ITAct 2000
343 Sec.82 of ITAct 2000
Power to give directions\textsuperscript{344}

It is prerogative of the Central Government to give directions to any State Government as to the carrying into execution in the State of any of the provisions of this Act or of any rule, regulation or order made there under.

Protection of action taken in good faith\textsuperscript{345}

It is clear vide this section that no suit, prosecution or other legal proceeding shall lie against the Central Government, the State Government, the Controller or any person acting on behalf of him, the Presiding Officer, adjudicating officers and the staff of the Cyber Appellate Tribunal for anything which is in good faith done or intended to be done in pursuance of this Act or any rule, regulation or order made there under.

Offences by companies\textsuperscript{346}

Section 85(1) of ITAct 2000 implies that where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

Section 85(2) of ITAct 2000 implies that despite of whatever contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be

\textsuperscript{344}Sec.81 of ITAct 2000  
\textsuperscript{345}Sec.84 of ITAct 2000  
\textsuperscript{346}Sec.85 of ITAct 2000
guilty of the contravention and shall be liable to be proceeded against and punished accordingly

**Removal of difficulties**\(^{347}\)

Section 86 (1) of ITAct 2000 implies that if any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as appear to it to be necessary or expedient for removing the difficulty provided that no order shall be made under this section after the expiry of a period of two years from the commencement of this Act.

Section 86(2) of ITAct 2000 implies that every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

**Power of Central Government to make rules**\(^{348}\)

Section 87(1) of ITAct 2000 implies that the Central Government may, by notification in the Official Gazette and in the Electronic Gazette make rules to carry out the provisions of this Act.

Section 87(2) of ITAct 2000 implies that in particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following mailers:

a) The manner and format in which any information may be authenticated (b) filing, issue, grant or payment (c) electronic records shall be filed, or issued (d) The matters relating to the type of digital signature (e) creating secure electronic record and secure digital signature (f) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers(g) Other standards to be observed by the Controller,(h) The requirements which an applicant must fulfill, (i) The period of validity of license granted (j) The form in which an application for license may be made (k) The amount of fees payable, (l) Such other documents which shall accompany an application for license, (m) The form and the fee for renewal of a license

\(^{347}\) Sec.86 of ITAct 2000

\(^{348}\) Sec.87 of ITAct 2000
and the fee payable there, (n) The form in which application for issue of a Digital Signature Certificate (o) The fee to be paid to the Certifying Authority for issue of a Digital Signature Certificate, (p) The adjudicating officer shall hold (q) The qualification and experience which the adjudicating officer shall possess (r) The salary, allowances and the other terms and conditions of service of the Presiding (s) The procedure for investigation of misbehavior or incapacity of the Presiding (t) The salary and allowances and other conditions of service of other officers and employees (u) The form in which appeal may be filed and the fee thereof, (v) Any other power of a civil court required to be prescribed (w) Any other matter which is required to be, or may be, prescribed. Section 87(3) of ITAct 2000 implies that every notification made by the Central Government under clause (f) of subsection (4) of section 1 and every rule made by it shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the notification or the rule or both Houses agree that the notification or the rule should not be made, the notification or the rule shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that notification or rule.

Constitution of Advisory Committee

Section 88 of ITAct 2000 implies that the Central Government shall, as soon as may be after the commencement of this Act, constitute a Committee called the Cyber Regulations Advisory Committee shall consist of a Chairperson and such number of other official and non-official members representing the interests principally affected or having special knowledge of the subject-matter as the Central Government may deem fit. It shall advise the Central Government either generally as regards any rules or for any other purpose connected with this Act; the Controller in framing the regulations under this Act and there shall be paid to the non-official members of such Committee

349 Sec.88 of ITAct 2000
such travelling and other allowances as the Central Government may fix. (Section 88 (1), (2) & (3) of IT Act 2000)

**Power of Controller to make regulations**

The Controller may, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government, by notification in the Official Gazette, make regulations consistent with this Act and the rules made there under to carry out the purposes of this Act. Such regulations may provide for all or any of the matters, i.e. a) the particulars relating to maintenance of data-base containing the disclosure record of every Certifying Authority, (b) The conditions and restrictions subject to which the Controller may recognize any foreign Certifying Authority, (c) the terms and conditions subject to which a license may be granted, (d) other standards to be observed by a Certifying Authority, (e) the manner in which the Certifying Authority shall disclose the matters, (f) the particulars of statement which shall accompany an application and (g) the manner in which the subscriber shall communicate the compromise of private key to the certifying Authority.

Every regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament and both Houses agree in making any modification in the regulation or both Houses agree, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that regulation. (Section 89 (1), (2) & (3) of IT Act 2000)

**Power of State Government to make rules**

The State Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.

The State Government may make rules regarding (a) the electronic form in which filing, issue, grant receipt or payment shall be effected under sub-section (1) of section 6; (b) for matters specified in sub-section (2) of section 6 and (c) any other matter which is required to be provided by rules by the State Government.

---

350 Sec. 89 of IT Act 2000
351 Sec. 90 of IT Act 2000
Every rule made by the State Government under this section shall be laid, as soon as may be after it is made, before each House of the State Legislature where it consists of two Houses, or where such Legislature consists of one House, before that House.

3.3.4(N) AMENDMENTS

SCHEDULE I

1) Amendments to the Indian Penal Code (45 Of 1860)\(^{352}\)

The Indian Penal Code shall be amended in the manner specified in the First Schedule to this Act.

First Schedule of Information Technology Act, 2000

1. After “Section 29”, the following section shall be inserted, namely “Section 29A”.

The words “electronic record” shall have the meaning assigned to them in clause (t) of sub-section (1) of section 2 of the Information Technology Act, 2000."

2. In section 167, for the words "such public servant, charged with the preparation or translation of any document, frames or translates that document", the words "such public servant, charged with the preparation or translation of any document or electronic record, frames, prepares or translates that document or electronic record" shall be substituted.

3. In section 172, for the words "produce a document in a Court of Justice", the words "produce a document or an electronic record in a Court of Justice" shall be substituted.

4. In section 173, for the words "to produce a document in a Court of Justice", the words "to produce a document or electronic record in a Court of Justice" shall be substituted.

5. In section 175, for the word "document" at both the places where it occurs, the words "document or electronic record" shall be substituted.

6. In section 192, for the words "makes any false entry in any book or record, or makes any document containing a false statement", the words "makes any false entry in any book or record, or electronic record or makes any document or electronic record containing a false statement" shall be substituted.

\(^{352}\) Sec.91 of IT Act 2000
7. In **section 204**, for the word "document" at both the places where it occurs, the words "document or electronic record" shall be substituted.

8. In **section 463**, for the words "Whoever makes any false documents or part of a document with intent to cause damage or injury", the words "Whoever makes any false documents or false electronic record or part of a document or electronic record, with intent to cause damage or injury" shall be substituted.

9. In **section 464**, for the portion beginning with the words "A person is said to make a false document" and ending with the words "by reason of deception practiced upon him, he does not know the contents of the document or the nature of the alteration", the following shall be substituted, namely "A person is said to make a false document or false electronic record"

10. In **section 466**, for the words "Whoever forges a document", the words "Whoever forges a document or an electronic record" shall be substituted.

11. In **section 468**, for the words "document forged", the words "document or electronic record forged" shall be substituted.

12. In **section 469**, for the words "intending that the document forged", the words "intending that the document or electronic record forged" shall be substituted.

13. In **section 470**, for the word "document" in both the places where it occurs, the words "document or electronic record" shall be substituted.

14. In **section 471**, for the word "document" wherever it occurs, the words "document or electronic record" shall be substituted.

15. In **section 474**, for the portion beginning with the words "Whoever has in his possession any document" and ending with the words "if the document is one of the description mentioned in section 466 of this Code", the following shall be substituted, namely: "Whoever has in his possession any document or electronic record, knowing the same to be forged and intending that the same shall fraudulently or dishonestly be used as a genuine, shall, if the document or electronic record is one of the description mentioned in section 466 of this Code."

16. In **section 476**, for the words "any document", the words "any document or electronic record" shall substituted.
17. In section 477A, for the words "book, paper, writing" at both the places where they occur, the words "book, electronic record, paper, writing" shall be substituted.

**SCHEDULE II**

2) Amendments to the Indian Evidence Act of 1872(1 Of 1872)\(^{353}\).

The Indian Evidence Act, 1872 shall be amended in the manner specified in the Second Schedule to this Act.

**Second Schedule of Information Technology Act, 2000**

1. In the definition of "Evidence", for the words "all documents produced for the inspection of the Court", the words "all documents including electronic records produced for the inspection of the Court" shall be substituted.

After the definition of "India", the following shall be inserted, namely: ‘the expressions "Certifying Authority", "digital signature", "Digital Signature Certificate", "electronic form", "electronic records", "information", "secure electronic record", "secure digital signature" and "subscriber" shall have the meanings respectively assigned to them in the Information Technology Act, 2000.’.

2. In section 17, for the words "oral or documentary", the words "oral or documentary or contained in electronic form" shall be substituted.

3. After section 22, the following section shall be inserted, namely "section22A”. Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question.”.

4. In section 34, for the words "Entries in the books of account", the words "Entries in the books of account, including those maintained in an electronic form" shall be substituted.

5. In section 35, for the word "record", in both the places where it occurs, the words "record or an electronic record" shall be substituted.

6. For section 39, the following section shall be substituted, namely "section39A” when any statement of which evidence is given forms part of a longer statement, or of a conversation or pan of an isolated document, or is contained in a document which forms part of a book, or is contained in part of electronic record or of a connected series

\(^{353}\) Sec.92 of IT Act 2000
of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, electronic record, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made."

7. After section 47, the following section shall be inserted, namely: "section 47A".

When the Court has form an opinion as to the digital signature of any person, the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact."

8. In section 59, for the words "contents of documents" the words "contents of documents or electronic records" shall be substituted.

9. After section 65, the following sections shall be inserted, namely 'section 65A. The contents of electronic records may be proved in accordance with the provisions of section 65B.

10. After section 67, the following section shall be inserted, namely "section67A". Except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the fact that such digital signature is the digital signature of the subscriber must be proved.".

11. After section 73, the following section shall be inserted, namely‘section73A”. In order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate; any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person..

12. After section 81, the following section shall be inserted, namely "section81 A”. The Court shall presume the genuineness of every electronic record purporting to be the Official Gazette, or purporting to be electronic record directed by any law to be kept by any person, if such electronic record is kept substantially in the form required by law and is produced from proper custody.".

13. After section 85, the following sections shall be inserted, namely "section85A”. The Court shall presume that every electronic record purporting to be an agreement
containing the digital signatures of the parties was so concluded by affixing the digital signature of the parties. Presumption as to electronic records and digital signatures.

Section 85B(1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

Section 85B (2) In any proceedings, involving secure digital signature, the Court shall presume unless the contrary is proved that (a) the secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record (b) except in the case of a secure electronic record or a secure digital signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature.

Section 85C. The Court shall presume, unless contrary is proved, that the information listed in a Digital Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber.

14. After section 88, the following section shall be inserted, namely “Section88A”. The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.

15. After section 90, the following section shall be inserted, namely ”section90A”. Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the digital signature which purports to be the digital signature of any particular person was so affixed by him or any person authorized by him in this behalf.

16. For section 131, the following section shall be substituted, namely”section131A”. No one shall be compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to refuse to produce if they were in his possession or control, unless such last-mentioned person consents to their production.”
**SCHEDULE III**

3) Amendments to the Banker’s Books Evidence Act 1891 (18 Of 1891)\(^{354}\).

The Bankers’ Books Evidence Act, 1891 shall be amended in the manner specified in the Third Schedule to this Act.

**Third Schedule of Information Technology Act, 2000**

1. In section 2(a) for clause (3), the following clause shall be substituted, namely clause (3)(a) “bankers’ books” include ledgers, day-books, cash-books, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device;

In section 2(b) for clause (8), the following clause shall be substituted, namely clause (8)(a) “certified copy” means when the books of a bank (a) are maintained in written form, a copy of any entry in such books together with a certificate written, the foot of such copy that it is a true copy of such entry, that such entry is contained in one of the ordinary books of the bank and was made in the usual and ordinary course of business and that such book is still in the custody of the bank, and where the copy was obtained by a mechanical or other process which in itself ensured the accuracy of the copy, a further certificate to that effect, but where the book from which such copy was prepared has been destroyed in the usual course of the bank’s business after the date on which the copy had been so prepared, a further certificate to that effect, each such certificate being dated and subscribed by the principal accountant or manager of the bank with his name and official title; (b) consist of printouts of data stored in a floppy, disc, tape or any other electro-magnetic data storage device, a printout of such entry or a copy of such printout together with such statements certified in accordance with the provisions of section 2A..

2. After **section 2**, the following section shall be inserted, namely: **section2A**. A printout of entry or a copy of printout referred to in sub-section (8) of section 2 shall be accompanied by the following, namely: (a) a certificate to the effect that it is a printout of

\(^{354}\) Sec.92 of IT Act 2000
such entry or a copy of such printout by the principal accountant or branch manager. (b) a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of.

(A) The safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorized persons.
(B) The safeguards adopted to prevent and detect unauthorized change of data.
(C) The safeguards available to retrieve data that is lost due to systemic failure or any other reasons.
(D) The manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electro-magnetic data storage devices.
(E) The mode of verification in order to ensure that data has been accurately transferred to such removable media.
(F) The mode of identification of such data storage devices.
(G) The arrangements for the storage and custody of such storage devices.
(H) The safeguards to prevent and detect any tampering with the system.
(I) Any other factor which will vouch for the integrity and accuracy of the system.
(J) A further certificate from the person in-charge of the computer system to the effect that to the best of his knowledge and belief, such computer system operated properly at the material time, he was provided with all the relevant data and the printout in question represents correctly, or is appropriately derived from, the relevant data.

SCHEDULE IV

4) Amendment to the Reserve Bank of India Act, 1934 (2 Of 1891)\(^{355}\).

Amendment to the Reserve Bank of India Act, 1934 (2 of 1934)

The Reserve Bank of India Act, 1934 shall be amended in the manner specified in the Fourth Schedule to this Act.

Fourth Schedule of Information Technology Act, 2000

In the Reserve Bank of India Act, 1934, in section 58, in sub-section (2), after clause (p), the following clause shall be inserted, namely Clause (pp) the regulation of fund transfer through electronic means between the banks or between the banks and other financial institutions referred to in clause (c) of section 45-1, including the laying down of

\(^{355}\) Sec.92 of IT Act 2000
the conditions subject to which banks and other financial institutions shall participate in such fund transfers, the manner of such fund transfers and the rights and obligations of the participants in such fund transfers”.

3.3.5 INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

3.3.5(A) BACKGROUND

Information technology is the maiden legislation in the country on information technology, computers and computers networks and e-commerce as well as e-communication. There were Act was the subject of detailed discussions, highly structured reviews and comprehensive criticisms. One segment of the industry called the IT Act 2000 as tough and very harsh as some section of the act are draconian in nature while on the other hand another segment of the industry always criticizing the Information Technology Act as too lenient and some people call the act as a lion with teeth.

There were prominent omissions in IT Act 2000 too and people repose their faith on the prevailing laws i.e. Indian Penal Code and therefore technology based cases were referred in IPC rather on the ITA. There was a demand for amendment since from its inception. Foremost industry bodies were discussed with and advisory groups were created to investigate the alleged lacunae in the I.T. Act 2000 and comparing it with similar legislations in other countries of the world and offer their recommendations on this front. The recommendations made by the advisory groups and other body corporate were examined and subsequently, the consolidated amendments to the Information Technology Act in the form of Information Technology Amendment Act 2008 was placed in the Parliament and passed at the end of 2008. The Amendment Act got the President assent on 5 Feb 2009 and was made effective from 27 October 2009.

Information Technology Amendment Act mainly focusing on Data privacy, Information Security, defining cyber crimes and cyber cafes, creating digital signature technology impartial, redefining reasonable security practices to be followed by corporate anda role of intermediaries, introducing and recognizing the role of Indian Computer Emergency Response Team[CERT-IN], includes some new additional cyber crimes like
child pornography and cyber terrorism and authorizing an Inspector to investigate cyber offences as against the DSP earlier by ITAct2000.

The Information Technology (Amendment) Bill, 2008 (Bill No.96-F of 2008) was passed by the both houses of parliament on December, 2008 and received the accent of the president on 5th February, 2009. However, the Information Technology (Amendment) Act, 2008 (ITAA, 2008) has been notified with effect from 27/10/2009 and starts its operations in India.

Many noteworthy amendments have been introduced in the IT Amendment Act, 2008:-

3.3.5(B) STRUCTURE OF THE INFORMATION TECHNOLOGY AMENDMENT ACT, 2008

The Act contains 4 Parts, 90 sections and 2 schedules.

Part-I contains Short title and commencement.
Part-II contains 90 sections
Part-III contains Amendments of the Indian Penal Code
Part-IV contains Amendment of the Indian Evidence Act, 1872
First Schedule – Documents or Transactions to which the Act shall not apply
Second Schedule – Electronic signature or Electronic authentication technique or procedure

[Last four sections namely sections 91 to 94 in the ITA 2000 were omitted and two new parts namely Part-III and Part IV were inserted]

3.3.6 INFORMATION TECHNOLOGY AMENDMENT ACT 2008

Part-I
(Preliminary)
1) Short title and commencement amended
   The short title and commencement amended as “This Act may be called the Information Technology (Amendment) Act, 2008”.
Part-II
2) Substitution of words “digital signature” by words “electronic signature”.
   In the Information Technology Act, 2000 (hereinafter in this Part referred to as the principal Act), for the words “digital signature” occurring in the Chapter, section,
subsection and clause referred to in the Table below, the words “electronic signature” shall be substituted.

Table3.12- The words “Electronic Signature” shall be substituted with “Digital Signature”

<table>
<thead>
<tr>
<th>S.N.</th>
<th>Chapter/section/sub-section/clause</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>clauses (d), (g), (h) and (zg) of section 2;</td>
</tr>
<tr>
<td>2</td>
<td>section 5 and its marginal heading;</td>
</tr>
<tr>
<td>3</td>
<td>marginal heading of section 6;</td>
</tr>
<tr>
<td>4</td>
<td>clauses (a), (b), (c) and (e) of section 10 and its marginal heading</td>
</tr>
<tr>
<td>5</td>
<td>heading of Chapter V;</td>
</tr>
<tr>
<td>6</td>
<td>clauses (f) and (g) of section 18;</td>
</tr>
<tr>
<td>7</td>
<td>sub-section (2) of section 19</td>
</tr>
<tr>
<td>8</td>
<td>sub-sections (1) and (2) of section 21 and its marginal heading</td>
</tr>
<tr>
<td>9</td>
<td>sub-section (3) of section 25;</td>
</tr>
<tr>
<td>10</td>
<td>clause (c) of section 30;</td>
</tr>
<tr>
<td>11</td>
<td>clauses (a) and (d) of sub-section (1) and sub-section (2) of section 34;</td>
</tr>
<tr>
<td>12</td>
<td>heading of Chapter VII;</td>
</tr>
<tr>
<td>13</td>
<td>section 35 and its marginal heading</td>
</tr>
<tr>
<td>14</td>
<td>section 64;</td>
</tr>
<tr>
<td>15</td>
<td>section 71;</td>
</tr>
<tr>
<td>16</td>
<td>sub-section (1) of section 73 and its marginal heading</td>
</tr>
<tr>
<td>17</td>
<td>section 74;</td>
</tr>
<tr>
<td>18</td>
<td>clauses (d), (n) and (o) of sub-section (2) of section 87</td>
</tr>
</tbody>
</table>

3. Amendment of section 1

In section 1 of the principal Act, for sub-section (4), the following sub-sections shall be substituted, namely Subsection (4) nothing in this Act shall apply to documents or transactions specified in the First Schedule, provided that the Central Government may, by notification in the Official Gazette, amend the First Schedule by way of addition or deletion of entries there to. Every notification issued under sub-section (4) shall be laid before each House of Parliament."

4. Amendment of section 2.

In section 2 of the principal Act after clause (h), the following clause shall be inserted, namely, clause (ha) “communication device” means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image; for clause (j), the following clause shall be substituted, namely, clause (j) “computer network” means the inter-connection of one or

356 Information Technology Amendment Act 2008
more computers or computer systems or communication device through the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and terminals or a complex consisting of two or more inter-connected computers or communication device whether or not the inter-connection is continuously maintained in clause (n), the word “Regulations” shall be omitted.

After clause (n), the following clauses shall be inserted, namely Clause (na) “cyber cafe” means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public; Clause (nb) “cyber security” means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction;

After clause (t), the following clauses shall be inserted, namely, clause(ta) “electronic signature” means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature; Clause (tb) “Electronic Signature Certificate” means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate.

After clause (u), the following clause shall be inserted, namely, clause (ua) “Indian Computer Emergency Response Team” means an agency established under sub-section (1) of section 70B. In clause (v), for the words “data, text”, the words “data, message, text” shall be substituted .For clause (w), the following clause shall be substituted, namely Clause (w) “intermediary”,

5. Amendment of heading of Chapter II.

In Chapter II of the principal Act, for the heading, the heading “DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE” shall be substituted.

6. Insertion of new section 3A Electronic signature

After section 3 of the principal Act, the following section shall be inserted, namely clause3A.

Notwithstanding anything contained in section 3, but subject to the provisions of sub-section a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which (a) is considered reliable; and (b) may be specified in the Second Schedule.
The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the Second Schedule provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable. Every notification issued under sub-section (4) shall be laid before each House of Parliament.

7. **Insertion of new section 6A. Delivery of services by service provider**

After section 6 of the principal Act, the following section shall be inserted, namely, section 6A.

The appropriate Government may, for the purposes of this Chapter and for efficient delivery of services to the public through electronic means authorize, by order, any service provider to set up, maintain and upgrade the computerised facilities and perform such other services as it may specify, by notification in the Official Gazette.

The appropriate Government may also authorize any service provider authorized under sub-section (7) to collect, retain and appropriate such service charges, as may be prescribed by the appropriate Government for the purpose of providing such services, from the person availing such service.

The appropriate Government shall, by notification in the Official Gazette, specify the scale of service charges which may be charged and collected by the service providers under this section.

8. **Insertion of new section 7A related to audit or documents, etc., maintained in electronic form.**

After section 7 of the principal Act, the following section shall be inserted, namely clause 7A. Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in the electronic form.

9. **Insertion of new section 10A related to validity of contracts formed through electronic means.**

After section 10 of the principal Act, the following section shall be inserted, namely Section 10A. Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case
may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.”.

10. Amendment of section 12.
In section 12 of the principal Act, in sub-section (1), for the words “agreed with the addressee”, the word “stipulated” shall be substituted

11. Substitution of new sections for sections 15 and 16
Secure electronic signature and Security procedures and practices
For sections 15 and 16 of the principal Act, the following sections shall be substituted, namely, section 15. An electronic signature shall be deemed to be a secure electronic signature if (i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and (ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed.

12. Amendment of section 17.
In section 17 of the principal Act (a) in sub-section (1), for the words “and Assistant Controllers”, the words “,Assistant Controllers, other officers and employees” shall be substituted; and (b) in sub-section (4), for the words “and Assistant Controllers”, the words “,Assistant Controllers, other officers and employees” shall be substituted.”.

Section 20 of the principal Act shall be omitted.

In section 29 of the principal Act, in sub-section (1), for the words “any contravention of the provisions of this Act, rules or regulations made there under”, the words “any contravention of the provisions of this Chapter” shall be substituted

15. Amendment of section 30.
In section 30 of the principal Act, in clause (c), after the word “assured”, the word “and” shall be omitted; after clause (c), the following clauses shall be inserted, namely Clause (ca) be the repository of all Electronic Signature Certificates issued under this Act; clause (cb) publish information regarding its practices, Electronic Signature Certificates and current status of such certificates.
16. Amendment of section 34.
In section 34 of the principal Act, in sub-section in clause (a), the words “which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate” shall be omitted.

17. Amendment of section 35.
In section 35 of the principal Act, in sub-section (4) the first proviso shall be omitted. In the second proviso, for the words "Provided further", the word "Provided" shall be substituted.

18. Amendment of section 36.
In section 36 of the principal Act, after clause (c), the following clauses shall be inserted, namely clause (ca) the subscriber holds a private key which is capable of creating a digital signature; clause (cb) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the subscriber.

19. Insertion of new section40A
Duties of subscriber of Electronic Signature Certificate
After section 40 of the principal Act, the following section shall be inserted, Namely section“40A. In respect of Electronic Signature Certificate the subscriber shall perform such duties as may be prescribed.”.

20. Amendment of heading of Chapter IX.
In Chapter IX of the principal Act, in the heading, for the words “PENALTIES AND ADJUDICATION”, the words “PENALTIES, COMPENSATION AND ADJUDICATION” shall be substituted.

21. Amendment of section 43.
In section 43 of the principal Act in the marginal heading, for the word “Penalty”, the words “Penalty and Compensation” shall be substituted; in clause (a), after the words “computer network”, the words “or computer resource” shall be inserted; after clause (h), the following clauses shall be inserted, namely“(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means; (j) steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;”; for the portion beginning with the words “he shall
be liable to pay damages” and ending with the words “persons so affected” the following shall be substituted, namely “he shall be liable to pay damages by way of compensation to the person so affected”; in the Explanation, after clause (iv), the following clause shall be inserted, namely “(v) “computer source code” means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

22. Insertion of new section 43A- Compensation for failure to protect data
After section 43 of the principal Act, the following section shall be inserted, Namely section 43A. Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

3. Amendment of section 46.
In section 46 of the principal Act in sub-section (1), for the words “direction or order made there under”, the words “direction or order made there under which renders him liable to pay penalty or compensation,” shall be substituted; after sub-section (1), the following sub-section shall be inserted, namely Subsection (1A). The adjudicating officer appointed under sub-section (1) shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees 5 crore provided that the jurisdiction in respect of the claim for injury or damage exceeding rupees five crore shall vest with the competent court. In sub-section (5), after clause (b) the following clause shall be inserted, namely Clause (c) shall be deemed to be a civil court for purposes of Order XXI of the Civil Procedure Code, 1908.

24. Amendment of heading of Chapter X.
In Chapter X of the principal Act, in the heading, the word “REGULATIONS” shall be omitted.

25. Amendment of section 48.
In section 48 of the principal Act, in sub-section (1), the word “Regulations” shall be omitted.
26. Substitution of new sections for sections 49 to 52.-Composition of Cyber Appellate Tribunal.

For sections 49 to 52 of the principal Act, the following sections shall be substituted, Namely
Section 49 The Cyber Appellate Tribunal shall consist of a Chairperson and such number of other Members, as the Central Government may, by notification in the Official Gazette, The selection of Chairperson and Members of the Cyber Appellate Tribunal shall be made by the Central Government in consultation with the Chief Justice of India. The Benches of the Cyber Appellate Tribunal shall sit at New Delhi and at such other places as the Central Government may, in consultation with the Chairperson of the Cyber Appellate Tribunal, by notification in the Official Gazette, specify the areas in relation to which each Bench of the Cyber Appellate Tribunal may exercise its jurisdiction. The Chairperson of the Cyber Appellate Tribunal may transfer a Member of such Tribunal from one Bench to another Bench.

Section 50 dealt with Qualifications for appointment as Chairperson and Members of Cyber Appellate Tribunal.

Section 51 dealt with Term of office, conditions of service, etc., of Chairperson and Members.

Section 52 dealt with the salary and allowances payable to the Chairperson or a Member of the Cyber Appellate Tribunal

Section 52A dealt with the powers of chairperson in respect of general superintendence and directions in the conduct of the affairs of that Tribunal

Section 52B. The Chairperson of the Cyber Appellate Tribunal may distribute the business of Tribunal amongst the Benches and matters to be dealt with by each Bench.

Section 52C. On the application of any of the parties and after notice to the parties, and after hearing such of them as he may deem proper to be heard, or suo motu without such notice, the Chairperson of the Cyber Appellate Tribunal may transfer any case pending before one Bench, for disposal to any other Bench.

Section 52D. If the Members of a Bench consisting of two Members differ in opinion on any point, they shall state the point or points on which they differ, and make a reference to the Chairperson of the Cyber Appellate Tribunal who shall hear the point or points and give the decision on the basis of the majority
27. Amendment of Section 53
In section 53 of the principal Act, for the words “Presiding Officer”, the words “Chairperson or Member, as the case may be,” shall be substituted.

28. Amendment of Section 54
In section 54 of the principal Act, for the words “Presiding Officer” wherever they occur, the words “Chairperson or the Member” shall be substituted.

29. Amendment of section 55
In section 55 of the principal Act, for the words “Presiding Officer”, the words “Chairperson or the Member” shall be substituted.

30. Amendment of Section 56
In section 56 of the Principal Act, for the words “Presiding Officer”, the word “Chairperson” shall be substituted.

31. Amendment of section 64.
In section 64 of the principal Act for the words “penalty imposed”, the words “penalty imposed or compensation awarded” shall be substituted and in the marginal heading, for the word “penalty”, the words “penalty or compensation” shall be substituted.

32. Substitution of new sections for sections 66 and 67
A) Section 66 enlarge the definition of cybercrime. Sections 66A – 66F define and impose penalties for other cyber crimes.

Sections 66A- Punishment for sending offensive messages through communication service, etc. shall be punishable with imprisonment for a term which may extend to three years and with fine.

Section 66B- Punishment for dishonestly receiving stolen computer resource or communication device shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to Rs.1 lakh or with both.

Section 66C- Punishment for identity theft shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to Rs.1 lakh.
Section 66D - Punishment for cheating by personation by using computer resource shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to Rs.1 lakh

Section 66E - Punishment for violation of privacy shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both

Section 66F - Punishment for cyber terrorism the amended legislation prescribing life imprisonment for such offences

B) Section 67 of the old Act is amended to reduce the term of imprisonment for publishing or transmitting obscene material in electronic form to three years from five years and increase the fine thereof from Indian Rupees 100,000 (approximately USD 2000) to Indian Rupees 500,000 (approximately USD 10,000).

The new sections have been inserted as Sections 67A to 67C.

Sections 67A - Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to Rs.10 lakh.

Section 67B - Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Section 67C - deals with the obligation of an intermediary to preserve and retain such information as may be specified for such duration and in such manner and format as the central government may prescribe.

33. Amendment of section 68

In section 68 of the principal Act, for sub-section (2), the following sub-section
shall be substituted, namely any person who intentionally or knowingly fails to comply with any order under sub-section shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or a fine not exceeding Rs.1 lakh both.”.

34. Substitution of Section 69

Section 69 empowers Central Government to designate agencies and issue direction for interception and safeguards for monitoring and decryption.

Section 69A dealt with Power to issue directions for blocking for public access of any information through any computer resource.

Section 69B dealt with the provision of Monitoring of Traffic Data and Information for Cyber Security is mentioned in So, the new amendments have strengthened the hands of the administration by increasing the ambit of the powers of interception of the Government.

35. Amendment of section 70.

Section 70 defines what is “Critical information infrastructure” which includes the computer resource. If any destruction causes to it not only has an adverse impact on security of India but it has also an impact on the economy, public health or safety of India. Our IT infrastructure is also be used to manage certain services offered to public at large, destruction of which may directly affect public health and safety. Hence, to maintain the security of Indian sovereignty, the protection of public health and safety is equally important.

36. Insertion of new sections 70A and 70B Establishment of National Nodal Agency.

By virtue of Section 70 A and Section B the Indian Computer Emergency Response Team, (CERT-In) has been appointed as the National nodal agency for critical information infrastructure protection. The CERT shall plays very important role to maintain the cyber security within the country. As per section 70B (6) coordination between CERTIn and service providers, data centers, body corporate and other persons should be maintained. CERTIn plays important roles in education, alert system, emergency response, issuing guidelines, reporting of cyber incident amongst other functions. It also excludes the court from taking cognizance of any offence under this
section except on a complaint made by authorized officer of CERTIn to prevent misuse of the Section

37. Insertion of new section 72A.

After section 72 of the principal Act, the following section shall be inserted, namely section 72A. It implies that an intermediary is required to act as per the terms of its lawful contract and not to disclose any personal information to cause wrongful loss or wrongful gain to any other person. It states that except as otherwise provided in the IT Act or any other law in force, if any person, including an intermediary, while providing services under the terms of a lawful contract, has secured access to any material containing personal information about another person, and with intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain, discloses the material to another person without the consent of the person concerned or in breach of a contract, then the person disclosing such information can be punished with imprisonment for up to 3 years and/or can be fined up to Rs. 5 lakh

38. Substitution of new sections for section 77.

For section 77 of the principal Act, the following sections shall be substituted, namely, section 77. No compensation awarded, penalty imposed or confiscation made under this act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force

Compounding of offences vide section 77A

Section 77A:-- A court of competent jurisdiction may compound offences, other than Offences for which the punishment for life or imprisonment for a term exceeding 3 Years have been provided, under this Act, provided that the court shall not compound such offence where the accused is, by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind. Provided further that the court shall not compound any offence where such offence affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or a woman. The person accused of an offence under this Act may file an application for compounding in the court in which offence is pending for trial and the provisions of sections 265B and 265C of the Code of Criminal Procedure, 1973 shall apply
Offences with 3 years’ imprisonment to be bailable under section 77B

Section 77B: Notwithstanding anything contained in the Code of Criminal Procedure, 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

39. Amendment of section 78.
In section 78 of the principal Act, for the words “Deputy Superintendent of Police” the word “Inspector” shall be substituted. The level of investigation brought down to the Inspectors from DSPs: *The level of investigation has been brought down to the level of inspector from that of DSP. It means, more IO’s are now available to investigate the cyber crime incidents.*

40. Substitution of new Chapters for Chapter XII.
For Chapter XII of the principal Act, the following Chapters shall be substituted,
Namely ‘CHAPTER XII Intermediaries not to be liable in certain cases.
Section 79 Exemption from liability of intermediary in certain cases: -
Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made hosted by him.

CHAPTER XIIA-EXAMINER OF ELECTRONIC EVIDENCE

Section 79A: - The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the Official Gazette, any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence where “electronic form evidence” means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines.

41. Amendment of section 80
In section 80 of the principal act, in sub-section (I), for the words “Deputy Superintendent of Police”, the word “Inspector” shall be substituted.
42 Amendment of section 81.
In section 81 of the principal Act, the following proviso shall be inserted at the end, Namely “Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957 or the Patents Act, 1970

43. Amendment of section 82.
In section 82 of the principal Act for the marginal heading, the following marginal heading shall be substituted,

A) “Chairperson, Members, officers and employees to be public servants
B) For the words “Presiding Officer”, the words “Chairperson, Members” shall be substituted

44. Amendment of section 84.
In section 84 of the principal Act, for the words “Presiding Officer”, the words “Chairperson, Members” shall be substituted

45. Insertion of new sections 84A, 84B and 84C
After section 84 of the principal Act, the following sections shall be inserted, namely:—

Section84A:-The Central Government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce, prescribe the modes or methods for encryption.

Section84B:-Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.

Explanation.—An act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.

Section84C:-Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of
imprisonment provided for that offence, or with such fine as is provided for the offence, or with both.

46. Amendment of section 87.
In section 87 of the principal Act, (A) in sub-section (2), various amendments were incorporated.

47. Amendment of section 90.
In section 90 of the principal Act, in sub-section (2), clause (c) shall be omitted.

48. Omission of sections 91, 92, 93 and 94.
Sections 91, 92, 93 and 94 of the principal Act shall be omitted.

49. For the First Schedule and the Second Schedule to the principal Act, the following Schedules shall be substituted,

“FIRST SCHEDULE [See sub-section (4) of section 1]
DOCUMENTS OR TRANSACTIONS TO WHICH THE ACT SHALL NOT APPLY :-
1. A negotiable instrument (other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881.
2. A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882.
3. A trust as defined in section 3 of the Indian Trusts Act, 1882.
4. A will as defined in clause (h) of section 2 of the Indian Succession Act, 1925, including any other testamentary disposition by whatever name called.
5. Any contract for the sale or conveyance of immovable property or any interest in such property.

SECOND SCHEDULE [See sub-section (l) of section 3 A]
Electronic Signature or Electronic Authentication Technique and Procedure

--------BLANK--------

50. Omission of Third Schedule and Fourth Schedule.
The Third Schedule and the Fourth Schedule to the principal Act shall be omitted
PART-III

51. Amendment of Indian Penal Code

In the Indian Penal Code

(a) In section 4, the word "offence" includes every act committed outside India which, if committed in India, would be punishable under this Code and the expression "computer resource" shall have the meaning assigned to it in clause (k) of sub-section (1) of section 2 of the Information Technology Act, 2000.

(b) In section 40, in clause (2), after the figure "117", the figures and word “118, 119 and 120” shall be inserted.

(c) In section 118, for the words “voluntarily conceals, by any act or illegal omission, the existence of a design”, the words “voluntarily conceals by any act or omission or by the use of encryption or any other information hiding tool, the existence of a design” shall be substituted.

(d) In section 119, for the words “voluntarily conceals, by any act or illegal omission, the existence of a design”, the words “voluntarily conceals by any act or omission or by the use of encryption or any other information hiding tool, the existence of a design” shall be substituted.

(e) In section 464, for the words “digital signature” wherever they occur, the words “electronic signature” shall be substituted.

PART-IV

52. Amendment of Indian Evidence Act.

In the Indian Evidence Act, 1872

(a) In section 3 relating to interpretation clause, in the paragraph appearing at the end, for the words “digital signature” and “Digital Signature Certificate”, the words “electronic signature” and “Electronic Signature Certificate” shall respectively be substituted;
(b) **Insertion of new section 45A** regarding opinion of Examiner of Electronic Evidence.

(c) **Amendment of section 47A:** In section 47A, (i) for the words “digital signature”, the words “electronic signature” shall be substituted; (ii) for the words “Digital Signature Certificate”, the words “Electronic Signature Certificate” shall be substituted;

(d) **Amendment of section 67A:** In section 67A, for the words “digital signature” wherever they occur, the words “electronic signature” shall be substituted

(e) **Amendment of section 85A:** In section 85A, for the words “digital signature” at both the places where they occur, the words “electronic signature” shall be substituted;

(f) **Amendment of section 85B:** In section 85B, for the words “digital signature” wherever they occur, the words “electronic signature” shall be substituted;

(g) **Amendment of section 85C:** In section 85C, for the words “Digital Signature Certificate”, the words “Electronic Signature Certificate” shall be substituted;

(h) **Amendment of section 90A:** In section 90A, for the words “digital signature” at both the places where they occur, the words “electronic signature” shall be substituted;

3.3.7 **BRIEF REVIEW OF CRITICAL ANALYSIS OF I.T. ACT, 2000 AND AMENDMENTS**

IT Act, 2000 gave the objectives namely to provide legal recognition for transactions carried out through electronic means, to facilitate the electronic filing of documents with government agencies and to amend certain Acts, among the other Acts are the Indian Penal Code, 1860, Indian Evidence Act, 1872. Critical evaluation of the IT Act 2000 reveals that it gave legal validity and recognition to electronic documents and digital signatures as per the preamble and objective of the Act. Similarly, to facilitate the electronic filing of documents with government agencies, Indian Penal Code 1860 and Indian Evidence Act 1872 were suitably amended. The Act with the formulation of the criminal and the civil liabilities for the infringement of the provisions of ITAct2000 also provided the regulatory regime to supervise the Certifying Authorities issuing digital signature certificates. IT Act 2000 granted a power to appoint adjudicating officer for the adjudicating the contravention of the Act. Due to the passage of the time new crimes were committed with the help of the information technology the need of the amendment of the Act felt to control the new cyber crimes by plug in the loopholes in the Act. In this
backdrop the Information Technology Amendment Act 2005 was passed by the parliament and made effective from 27 October 2009. The ITAA 2008 conveyed noticeable changes in the IT Act, 2000 as under:-

1) Section 70 B of ITAA 2008 has provided the Powers to intercept monitor and block websites has been introduced by IT Amendment Act 2008 The Indian Computer Emergency Response Team as a National Nodal Agency nominated by the Government of India.

2) Liability of intermediaries and the concept of Due Diligence have been introduced in Section 79 of ITAA2008. After passing the act of Due Diligence by ITAA and the introduction of ‘reasonable security practices and procedures’ and the responsibility of body corporate as seen earlier in Section 43A, the DIT came out with a set of rules titled Information Technology (Intermediaries Guidelines) Rules on 11 April 2011 to avoid the confusion.

3) Penalty for breach of confidentiality and privacy is discussed in Section 72 with the punishment being imprisonment for a term up to two years or a fine of one lakh rupees or both,

4) Section 75 clearly states that the Act is applicable to contravention committed outside India, if the contravention involves a computer or a computer network located in India.

5) Provisions were made only for compounding of contraventions and not for offences under Chapter XI of the IT Act. Now, the provision for compounding of offences under the IT Act has been made under the newly inserted Section 77-A of IT AA, 2008. However, it is to be noted that under the amendment, the second conviction is not compoundable and it also not compoundable where such offence affects the socio-economic conditions of the country or has been committed against a child below the age of 18 years or a woman

6) ITA 2000 has amended the sections dealing with records and documents in the IPC by inserting the word ‘electronic’ thereby treating the electronic records and documents at par with physical records and documents. The Sections dealing with false entry in a record or false document etc (eg 192, 204, 463, 464, 464,
468 to 470, 471, 474, 476 etc) have since been amended as electronic record and electronic document thereby bringing within the ambit of IPC.

7) The Indian Evidence Act 1872 is another legislation amended by the ITA. Prior to the passing of ITA, all evidences in a court were in the physical form only. With the ITA giving recognition to all electronic records and documents. Admissibility of electronic records as evidence as preserved in Section 65B of the Act assumes significance.

8) Amendment to the Bankers’ Books Evidence (BBE) Act 1891 has been included as the third schedule in ITA2000. Prior to the passing of ITA, any evidence from a bank to be produced in a court, necessitated production of the original ledger or other register for verification at some stage with the copy retained in the court records as exhibits.

9) The Reserve Bank of India Act, 1934 was amended by the ITA2000. Section 58 of the Act sub-section (2), after clause (p), a clause relating to the regulation of funds transfer through electronic means between banks.

10) The role of Adjudicating Authority in the amended Act is very significant. The subject matter of its jurisdiction, adjudging matters alleging contravention and awarding compensation under chapter 9 is explained in clearer terms in the Amended IT Act. The amended Act also curtails the power & jurisdiction of the Adjudicating officers and excludes those matters where compensation claimed is more than 5 crore.

11) The corporate responsibility for data protection is incorporated in S 43A in the amended IT Act, 2000 whereby corporate bodies handling sensitive personal information or data in a computer resource are under an obligation to ensure adoption of ‘reasonable security practices’ to maintain its secrecy, failing which they may be liable to pay damages.

12) The role of the Controller to act as repository of digital signatures has been repealed by the IT Amendment Act, 2008. This role has now been assigned to the Certifying Authority in Section 30 of the IT Act.

13) The amended Act has changed the composition of the Cyber Appellate Tribunal. The Presiding officer alone would earlier constitute the Cyber Regulations
Appellate Tribunal which provision has now been amended. The tribunal would now consist of Chairperson and such number of members as Central Government may appoint.

14) New cybercrimes as offences under amended Act-

Many cybercrimes for which were not covered under the IT Act, 2000 included by the IT (Amendment) Act, 2008 as under:

a) Sending of offensive or false messages (s 66A),

b) Receiving stolen computer resource (s 66B),

c) Identity theft (s 66C), cheating by personation (s 66D),

d) Violation of privacy (s 66E).

e) A new offence of Cyber terrorism is added in Section 66 F which stipulated punishment that may extend to imprisonment for life. Section 66 F covers any act committed with intent to threaten unity, integrity, security or sovereignty of India or cause terror by causing DoS attacks, introduction of computer contaminant, unauthorized access to a computer resource, stealing of sensitive information, any information likely to cause injury sovereignty and integrity of India,

f) For other offences mentioned in Section 66, punishment prescribed is generally up to three years and fine of one/two lakh has been prescribed and these offences are cognizable and bailable.

g) Further, as per new S. 84 B, abetment to commit an offence is made punishable with the punishment provided for the offence under the Act and the new Section 84 C makes attempt to commit an offence also a punishable offence with imprisonment for a term which may extend to one-half of the longest term of imprisonment provided for that offence.

h) In certain offences, such as hacking (s 66) punishment is enhanced from 3 years of imprisonment and fine of 2 lakh to fine of 5 lakh.

i) In Section 67 for publishing of obscene information imprisonment term has been reduced from five years to three years (and five years for subsequent offence instead of earlier ten years) and fine has been
increased from one lakh to five lakh (rupees ten lakh on subsequent conviction).

j) Section 67A adds an offence of publishing material containing sexually explicit conduct punishable with imprisonment for a term that may extend to 5 years with fine up to ten lakh.

k) Sections 67B punish offence of child pornography, child’s sexually explicit act or conduct with imprisonment on first conviction for a term up to 5 years and fine up to 10 lakh. This is a positive change as it makes even browsing and collecting of child pornography a punishable offence.

l) Punishment for disclosure of information in breach of lawful contract under section 72 is increased from 2 yrs up to 5 yrs and from one lakh to 5 lakh or both. This will deter the commission of such crime.

m) By virtue of Section 84 B person who abets a cybercrime will be punished with punishment provided for that offence under the Act.

n) Also, punishment for attempt to commit offences is given under Section 84 c which will be punishable with one half of the term of imprisonment prescribed for that offence or such fine as provided or both.

15. Section 67C to play a significant role in cyber crime prosecution Any intermediary that contravenes this provision intentionally or knowingly shall be liable on conviction for imprisonment for a term not exceeding 2 yrs or fine not exceeding one lakh or both.

16. Section 66 E elaborates about acts of intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

17. Section 68(2), to deals with the direction of controller punishable with three years of imprisonment or fine of two lacks or both now, has been reduced to two years punishment or fine of one lakh of rupees or both.
18. Section 69 that deals with power of Controller to intercept information being transmitted through a computer resource when necessary in national interest is amended by Section 69.

i) Section 69A has been inserted in the IT Act by the amendments in 2008 and gives power to Central government or any authorized officer to direct any agency or intermediary (for reasons recorded in writing) to block websites in special circumstances as applicable in Section 69. Under this Section the grounds on which such blocking is possible are quite widen

ii) Section 69B added to confer Power to collect, monitor traffic data by the agencies appointed by the Central Government

19. It provides that the Intermediary shall be liable if he has conspired or abetted or induced, whether by threats or promise or otherwise in the commission of the unlawful act (Section 79(3)(a)).

20. The Section 78 of the Act is amended to confer power to investigate offences under the Act from DSP level to Inspector level.

21. Section 79 A is added that empowers the Central government to appoint any department or agency of Central or State government as Examiner of Electronic Evidence.

3.3.8. GREY AREAS IN ITA 2000 AND ITAA2008

Information Technology Act 2000 and Amendment Act 2008 has following grey areas

Though, Information Technology Act, 2000, itself is a comprehensive legislation but it has had some inbuilt shortcomings. With the new amendment act 2008 it is hope that various trouble and problems in real cyber world will be determined. Some new acts were introduced as explained above. By adding the new definitions and removing the wording in some sections of the act to remove the confusion was the welcome attempt on the part of the government.

On the basis of the critical evolution of the IT Act 2000 & IT Amendment Act 2008 in the foregoing paragraphs it is observed that there are some grey areas in the Act which need special concentration as under:-
1) **Jurisdiction is not satisfactorily addressed in the ITA2000 and ITAA2008.**

The cyber space doesn’t know any boundaries. Cyber crimes committed by the miscreants is geography-agnostic, borderless, territory-free and observe no jurisdiction and frontiers are happens in virtual space. It has been mentioned about the jurisdiction in Sections 46, 48, 57 and 61 in the context of adjudication process and the appellate procedure. In Section 80 and as part of the police officers’ powers to enter, search a public place for a cyber crime etc. In the context of electronic record, Section 13 (3) and (4) discuss the place of dispatch and receipt of electronic record which may be taken as jurisdictional issues. The Act extends the application of its penal provisions to persons outside India, irrespective of their nationality if the offence under the Act relates to a computer located in India. There are limitations of enforcement of provisions of law against such extra-territorial jurisdiction. The jurisdiction of a particular country over online transactions, which involves multiple jurisdictions, is not addressed properly by the Act. Similarly, the IT Act is silent on the important issue of in respect of deciding the place and police station for filing and registering the case.

2) **Many cyber crimes are left uncovered under ITAct**

Many cyber crimes like cyber squatting with an evil intention to extort money. Spam mails, ISP’s liability in copyright infringement, Data privacy issues, Chat room abuse, Money laundering and watching pornography on internet have not been given adequate coverage.

3) **There is no provision for ‘Spam’ while ‘Phishing’ is not addressed in a comprehensive manner.**

Spam is undesired and unsolicited bulk e-mail. In the current days it reflects the major economic problems. Stringent legislation is required to deal with the problem of spam. The laws for the prevention of spam in India are missing as the IT Act, 2000 fails to address this issue. Another major failure of ITAA2008 is the Act has not dealt with the entire issue pertaining to spam in a comprehensive manner. In any case, the word spam is not even mentioned anywhere in the IT Amendment Act. Similarly Phishing is typically carried out by e-mail and often directs users to enter personal and financial details at a website. The IT Act 2000, however, does not specifically define phishing as
an offence and thus the law enforcement authorities have to take recourse to the
generic provisions of cheating and criminal breach of trust under the Indian Penal Code.
Section 66 A addressed sending of menacing, annoying messages and also misleading
information about the origin of the message not compressively addressed ‘Phishing’

4) The Act fails to cover cyber squatting.
Cyber squatting is the act of registering a popular internet domain address that is likely
to be wanted by another person, business, or organization in the hope that it can be
sold to them for a profit with an evil intention to online extortion..cyber squatters register
trade-marks, trade names, business names and so on, belonging to third parties with
the common motive of trading on the reputation and goodwill of such third parties by
either confusing customers or potential customers, and at times, to even sell the domain
name to the rightful owner at a profit. In India there is no Domain Name Protection
Law and cyber squatting cases are decided under Trade Mark Act, 1999.Once
again the ITA and ITAA fails to cover such important problem of cyber squatting.

5) Prevention of Money Laundering Act not comprehensively addressed.
After the passing of the Rule in April 2011, on the “Reasonable Security Practices and
Procedures” as part of ITAA 2008 and Section 43A of ITAA, banks should strive well to
prove that they have all the security policies in place like compliance with ISO 27001
standards etc and e-records are maintained. The Act has not covered the issues of
Money Laundering comprehensively.

6) Privacy & Data Protection in Internet banking not addressed adequately.
Privacy and data protection are important issues that need to be addressed by the
Information Technology Act. Internet Banking involves not just the banks and their
customers, but numerous third parties too. There is an exchange of Information held
by banks about their customers on several times. There is a high risks in preventing
leakage or tampering of data of the customers. India has no law on data protection.
The Information Technology Act talks about unauthorized access but it does not talk
about maintaining integrity of customer transactions. The act does not mandate any
responsibility upon banks to protect the details of customers and clients. Similarly
issues related to privacy is of utmost importance today if not an entire act can be
brought into force, then at least specific provisions relating to privacy and data protection be incorporated into the Act

7) Awarding punishment by the Cyber Appellate Tribunal can be challenged on the ground of its defective constitution

The amended Act has changed the composition of the Cyber Appellate Tribunal. The tribunal would now consist of Chairperson and such number of members as Central Government may appoint. The decision making process allows more objectivity with Section 52 D that provides that the decision shall be taken by majority. It is pertinent to note that there has not been any amendment in Section 55 by 2008 amendments which states that no order of CAT shall be challenged on ground that there existed a defect in constitution of appellate tribunal.

8) Combined effect of Section 78 & 80 may misused easily

By virtue of Section 78 of the Act, the power to investigate offences under the Act from DSP level to Inspector level. Section 80 has been amended and power to enter and search in a public place is now vested in any police officer not below the rank of inspector or any authorized officer of central government or state government. The section empower the officer to arrest without warrant a person found therein who is reasonably suspected of having committed or of committing or being about to commit any offence under this Act. There is no provision in this section that unless it is reasonably suspected that a person has committed, is committing or is about to commit an offence, he should not be arrested without warrant.

9) Liability of Intermediary amended without direction

The section 79 of ITA2000 hold network service providers liable for third party content only when the service provider failed to prove that the crime was committed without his knowledge or he failed to prove that he had exercised due diligence to prevent the offence or contravention. The burden of proof was on the network service provider. However, no such directions are given to intermediary to install any appropriate software to expeditiously remove or disable access to the unlawful material without vitiating the evidence in any manner.
10) There is no provision for creating awareness in the Act.
The investigating agencies and law enforcement agencies have not taken any serious step to create public awareness about the provisions in these legislations, which is extremely important bearing in mind that this is a new area and technology has to be learnt by all the stake-holders like the judicial officers, legal professionals, litigant public and the public or users at large. There is no such provision made in the Act.

11) Appointment of Examiner of Electronic Evidence but no provisions for cyber evidence in the IT Act
With amendments in 2008, Section 79 A is added that empowers the Central government to appoint any department or agency of Central or State government as Examiner of Electronic Evidence. This agency will play a crucial role in providing expert opinion on electronic form of evidence. No comprehensive provision for cyber evidence is there.

12) There is no provision in terms of e-mail and its value as an evidence in the Act
IT Act does not describes anything about e-mail and its authenticity or its legal value as an evidence to be produced in the court of laws

13) The Act does not address the issue of protection of intellectual property
In section 81 of the principal Act, the following provision inserted at the end, namely “Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957 or the Patents Act, 1970. The act is silent provided the protection of Intellectual Property Rights i.e. copy right, trade mark, patents etc. in the electronic form.

14) Act is silent about the domain names infringement
There is no provision in the ITA 2000 and ITAA2008 on domain names infringement. However entire e-commerce is principally based on the domain name and in turn Information Technology Act 2000 was came into existence to support the e-commerce activities in India.
15) The Act fails to address the issue of cross-border taxation that may arise in international contracts
Due to the advent of Information Technology, International Trade gains the prime importance. For this purpose, international contracts required to be signed. Taxation policies of the government are formulated to generate the revenue. However, this Act silent on the cross-border taxation policy.

16) Combined effect of Section33 & 77B on non surrender of license by Certifying Authority
As per the provisions of Section 33 of the IT Act 2000, when a license of the certifying authority is suspended or revoked then the certifying authority have to surrender the license to controller compulsorily. In case certifying authority fails to surrender the license then he shall be punished with imprisonment which may extend up to 6 months or a fine which may extend to Rs. 10,000 or both. The provisions of Section 77B of ITAA 2008 any offence punishable with imprisonment of 3 years or above shall be termed as cognizable offence. In the light of the section 77B failure to surrender license u/s 33 is a non-cognizable offence which is serious lapses on the part of the Certifying Authority.

17) Important documents are not covered under IT Act.
As per section1 of ITAct 2000 Important documents such as ‘Power of Attorney’(Sec 1 of the Attorney Act,1882),’Trust deed’(Sec.3 of Indian Trust Act,1882),’ Will’(Sec.2h,of Indian succession Act,1925) and Contract for the sale or conveyance of immovable property or any interest in such property are not covered under this Act.

18) Act doesn’t provide any parameter for implementation.
This Act doesn’t systematically lays down any parameters for its implementation. The Stake holders of the law enforcement agency like police, judges are not computer savvy
19) Statutory Bodies may not accept Electronic Documents
As per Section 9 of IT Act, no one can persist any government office to interact in electronic form. Therefore statutory bodies not bounded to accept electronic documents

20) Government Policy on Utility software or System software not addressed by the Act
Many Indian Corporate Houses including Public Sector Under Takings and Public Sector Banks use Operating Systems that are from the West especially the United States of America. These Corporate Houses and PSU’s and PSB’s imports many software utilities and hardware items and sometimes firmware are from abroad. To avoid the peculiar situation when the user is not confident about the status of upgraded or patch is either getting downloaded or any spyware is getting installed then In such cases, the actual reach and import of IT Act Sections dealing with a utility software or a system software or an Operating System upgrade or update used for downloading the software utility, is to be specifically addressed. The Act is silent on government’s policy on keeping the backup of corporate including the PSUs and PSBs in our county or abroad the subjective legal jurisprudence on such software backups.357

21) Following loop holes are also required to be plug in by the IT Act
   1) Adequate coverage for liability in copyright infringement, not given
   2) Misuse of Digital Signature

*******

3.4 PROBLEMS OF LAW TO CONTROL CYBER CRIMES AGAINST E-BANKING IN INDIA

The information technology is used as multipurpose vehicle, which can be used for negative as well as positive work. Thus, the outcomes of many projects rely on the technology user in what way the technology is being used by the user. It depends on the intension of the user whether it is used with judicious or malicious intentions. Phishing, hacking, spamming, malware, data theft, virus attack, Trojans etc. are the examples of offenses committed with a malicious intention by using the information technology. Such types of offenses are the example of cyber crimes and misuse of the information technology. These cyber crimes are creating the havoc and nuisance in the cyber world in general and in banking industry in particular.

3.4.1 E- BANKING PROBLEMS AND LEGAL REMEDIES
Hon’ble Justice K.G. Balkrishnan, Chief Justice of India in the conference held at New Delhi on January 31st 2010 on National Consultation on Enforcement of Cyber Law addressed as under:

“*The expanding reach of computers and the internet has made it easier for people to keep in touch across long distance and collaborate for purpose related to business, education and culture among others. However the means that enable the free flow of information across borders also gives rise to worryingly high incidence of irresponsible behaviour. Any technology is capable of beneficial use as well as misuse. It is the job of the legal system and regulatory agencies to keep pace with the same and ensure that newer technologies do not become tools of exploitation and harassment.*“

---

358 Hon’ble Justice K.G. Balkrishnan, Chief Justice of India in the conference held at New Delhi on January 31st 2010 on National Consultation on Enforcement of Cyber Law
The open architecture of the Internet exposes the banks’ systems to decide access through the easy availability of technology. The legal framework for banking in India is provided by a set of enactments, viz., the Banking Regulations Act, 1949, the Reserve Bank of India Act, 1934, and the Foreign Exchange Management Act, 1999. Besides these, banking activity is also influenced by various enactments governing trade and commerce, such as, Indian Contract Act, 1872, the Negotiable Instruments Act, 1881, Indian Evidence Act, 1872, etc. Internet banking is an extension of the traditional banking, which uses Internet both as a medium for receiving instructions from the customers and also delivering banking services. Hence, conceptually, various provisions of law, which are applicable to traditional banking activities, are also applicable to Internet banking.

Government of India has enacted The Information Technology Act, 2000, in order to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication. The Act has also amended certain provisions of the Indian Penal Code, the Indian Evidence Act, 1872, The Bankers Book of Evidence Act, 1891 and Reserve Bank of India Act 1934 in order to facilitate ecommerce in India.359

There is also the question of adequacy of law to deal with situations which are technology driven like denial of service / data corruption because of technological failure, infrastructure failure, spreading viruses & worms, Trojan horse, website compromise and Malware Propagation, Denial of Service (DoS)/ Distributed Denial of Service (DDoS), phishing/ vishing attack, hacking, spamming, network scanning/probing, money laundering, fiscal frauds and other cyber crimes perpetrated against bank like carders and internet search engine/Google “hacking”

Cross border transactions carried through Internet pose the issue of jurisdiction and conflict of laws of different nations. Problem of Extra territorial jurisdiction & extradition of offenders is also important in the internet banking. There are certain things in the physical form of evidence which cannot be applied to Internet evidence and when applied it would be almost impossible to admit computer evidence. Therefore problems related with obtaining evidence in electronic form are the burning issue in the electronic

359 ITAct,2000
banking. Other major problems of law faced by the banking industry are data theft and cyber terrorism related with banking.

The cyber laws in force in the country are, Indian Penal Code (IPC), Information Technology Act 2000, Information Technology Amendment Act 2008, Data Protection Act, Criminal Procedure Code, Indian Evidence Act, etc. These laws are lacking in enforceability. Due to several Laws dealing with the problem lays confusion as to their applicability, and none of the Law deals with the problem specifically in total. Although these legislations talk about the problem but they don’t provide an end to it. Due to inefficiency of the existing laws in their enforceability creates the problems of law to control the cyber crime against electronic banking in India.

At present the banking industry is facing the major problems of mounting number of cyber crimes due to inefficiency of the cyber laws. Other problems of law faced by the banking industry are data theft, cyber terrorism, jurisdictional and extraterritorial problems and problem of electronic evidence.

3.4.2 (I) PROBLEM OF MOUNTING INCIDENTS OF CYBER CRIMES AGAINST E-BANKING IN INDIA.

Cyber-Crimes commonly perpetrated against banks

Many terms are in vogue in the present scenario of hi-tech crimes viz, ‘digital crime’, ‘computer crime’ and ‘cyber crime’. Sometimes these terms are also used interchangeably. The terms electronic crime is the synonyms of computer crime, e-crime and cyber-crime. E-crime is broadly used to describe a crime that involves computers or other such electronic devices are used either as a tool to commit the crime, as a storage device, or as a target of the crime. Computers are used as a storage device. This information is retrieved and used for committing the crime by an illegal access to the computers by the miscreants. An example in this category is stolen

intellectual property. When the computers are used as a target of crime and if the information which is stored in those computers is changed by using the criminal means and recovered in an illegal way, such crimes can be termed as either electronic crimes or cyber crimes ranging from hacking to phishing.

**Cyber-crimes commonly committed against banks are as under:-**

1) Spreading Viruses & Worms  
2) Trojan horse  
3) Website Compromise and Malware Propagation  
4) Denial of Service (DoS)/ Distributed Denial of Service (DDoS)  
5) Phishing/ Vishing attack  
6) Hacking  
7) Spamming  
8) Network Scanning/Probing  
9) Money Laundering  
10) Fiscal Fraud  
11) Other Cyber Crimes against Bank are Carders and Internet Search Engine/Google hacking

i) **THE ASIA PACIFIC COMPUTER EMERGENCY RESPONSE TEAM (APCERT)**

The Asia Pacific Computer Emergency Response Team (APCERT) is a coalition of Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) within the Asia Pacific region. The organization was established in February 2003 with the objective of encouraging and supporting the activities of CERTs/CSIRTs in the region.

ii) **APCERT MEMBERS**

APCERT was formed in 2003 by 15 teams from 12 economies across the Asia Pacific region, and its membership has continued to increase since then. As of December 2012, APCERT consists of 30 teams from 20 economies across the Asia Pacific region, of which 21 teams are Full Members and 9 teams are General Members.

---

361 Source: Annual Report of Asia Pacific Computer Emergency Response Team (2012)
### a) Full Members (21 Teams)

<table>
<thead>
<tr>
<th>Team</th>
<th>Official Team Name</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>AusCERT</td>
<td>Australian Computer Emergency Response Team</td>
<td>Australia</td>
</tr>
<tr>
<td>BKIS</td>
<td>Bach Khoa Internetwork Security Center</td>
<td>Vietnam</td>
</tr>
<tr>
<td>BruCERT</td>
<td>Brunei Computer Emergency Response Team</td>
<td>Negara Brunei Darussalam</td>
</tr>
<tr>
<td>CCERT</td>
<td>CERNET Computer Emergency Response Team</td>
<td>People's Republic of China</td>
</tr>
<tr>
<td>CERT Australia</td>
<td>CERT Australia</td>
<td>Australia</td>
</tr>
<tr>
<td>CERT-In</td>
<td>Indian Computer Emergency Response Team</td>
<td>India</td>
</tr>
<tr>
<td>CNCERT(CC)</td>
<td>National Computer network Emergency Response technical Team / Coordination Center of China</td>
<td>People's Republic of China</td>
</tr>
<tr>
<td>HKCERT</td>
<td>Hong Kong Computer Emergency Response Team / Coordination Centre</td>
<td>Hong Kong, China</td>
</tr>
<tr>
<td>ID-CERT</td>
<td>Indonesia Computer Emergency Response Team</td>
<td>Indonesia</td>
</tr>
<tr>
<td>ID-SIRTII</td>
<td>Indonesia Security Incident Response Team of Internet Infrastructure</td>
<td>Indonesia</td>
</tr>
<tr>
<td>JPCERT(CC)</td>
<td>Japan Computer Emergency Response Team / Coordination Center</td>
<td>Japan</td>
</tr>
<tr>
<td>KrCERT(CC)</td>
<td>Korea Internet Security Center</td>
<td>Korea</td>
</tr>
<tr>
<td>MyCERT</td>
<td>Malaysian Computer Emergency Response Team</td>
<td>Malaysia</td>
</tr>
<tr>
<td>PHCERT</td>
<td>Philippine Computer Emergency Response Team</td>
<td>Philippine</td>
</tr>
<tr>
<td>SingCERT</td>
<td>Singapore Computer Emergency Response Team</td>
<td>Singapore</td>
</tr>
<tr>
<td>Sri Lanka CERT</td>
<td>Sri Lanka Computer Emergency Readiness Team Coordination Centre</td>
<td>Sri Lanka</td>
</tr>
<tr>
<td>ThaiCERT</td>
<td>Thailand Computer Emergency Response Team</td>
<td>Thailand</td>
</tr>
<tr>
<td>TechCERT</td>
<td>TechCERT</td>
<td>Sri Lanka</td>
</tr>
<tr>
<td>TWCCERT/CC</td>
<td>Taiwan Computer Emergency Response Team / Coordination Center</td>
<td>Chinese Taipei</td>
</tr>
<tr>
<td>TWNCERT</td>
<td>Taiwan National Computer Emergency Response Team</td>
<td>Chinese Taipei</td>
</tr>
<tr>
<td>VNCERT</td>
<td>Vietnam Computer Emergency Response Team</td>
<td>Vietnam</td>
</tr>
</tbody>
</table>

Source: Annual Report of Asia Pacific Computer Emergency Response Team (2012)
b) General Members (9 Teams)

Table 3.14-General Members of Asia Pacific Computer Emergency Response Team APCERT

<table>
<thead>
<tr>
<th>Team</th>
<th>Official Team Name</th>
<th>Economy</th>
</tr>
</thead>
<tbody>
<tr>
<td>BDCERT</td>
<td>Bangladesh Computer Emergency Response Team</td>
<td>Bangladesh</td>
</tr>
<tr>
<td>BP DSIRT</td>
<td>BP Digital Security Incident Response Team</td>
<td>Singapore</td>
</tr>
<tr>
<td>EC-CERT</td>
<td>Taiwan E-Commerce Computer Emergency Response Team</td>
<td>Chinese Taipei</td>
</tr>
<tr>
<td>GCSIRT</td>
<td>Government Computer Security and Incident Response Team</td>
<td>Philippines</td>
</tr>
<tr>
<td>mmCERT</td>
<td>Myanmar Computer Emergency Response Team</td>
<td>Myanmar</td>
</tr>
<tr>
<td>BDCERT</td>
<td>Bangladesh Computer Emergency Response Team</td>
<td>Bangladesh</td>
</tr>
<tr>
<td>BP DSIRT</td>
<td>BP Digital Security Incident Response Team</td>
<td>Singapore</td>
</tr>
<tr>
<td>EC-CERT</td>
<td>Taiwan E-Commerce Computer Emergency Response Team</td>
<td>Chinese Taipei</td>
</tr>
<tr>
<td>GCSIRT</td>
<td>Government Computer Security and Incident Response Team</td>
<td>Philippines</td>
</tr>
</tbody>
</table>

COMPUTER EMERGENCY RESPONSE TEAMS INDIA (CERT-In)

CERT-In is a functional organization of Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India, with the objective of securing Indian cyber space. CERT-In provides Incident Prevention and Response services as well as Security Quality Management Services. The Information Technology Act, 2000 designated CERT-In to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents

CERT-In is operational since January, 2004. The constituency of CERT-In is the Indian cyber community. CERT-In works closely with the Chief Information Security Officers and System Administrators of various sectoral and organizational networks of its constituency.

Source: Annual Report of Asia Pacific Computer Emergency Response Team (2012)
3.4.3 CYBER CRIME INCIDENTS AGAINST E-BANKING HANDLED BY CERT INDIA

In the year 2012, CERT-In handled more than 22000 incidents. The types of incidents handled were mostly of Spam, Website compromise & malware propagation, Malicious Code, Phishing and Network Scanning & Probing.

Table 3.15- The year-wise summary of cyber crime incidents against e-banking (Amt in Crore)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Cyber Security Incidents</td>
<td>23</td>
<td>254</td>
<td>552</td>
<td>1237</td>
<td>2565</td>
<td>8266</td>
<td>10315</td>
<td>13301</td>
<td>22060</td>
</tr>
<tr>
<td>Virus and Malicious Code</td>
<td>5</td>
<td>95</td>
<td>19</td>
<td>358</td>
<td>408</td>
<td>596</td>
<td>2817</td>
<td>2765</td>
<td>3149</td>
</tr>
<tr>
<td>Website Compromise and Malware Propagation</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>835</td>
<td>6548</td>
<td>6344</td>
<td>4394</td>
<td>4591</td>
</tr>
<tr>
<td>Phishing</td>
<td>3</td>
<td>101</td>
<td>339</td>
<td>392</td>
<td>604</td>
<td>374</td>
<td>508</td>
<td>674</td>
<td>887</td>
</tr>
<tr>
<td>Network Scanning/Probing</td>
<td>11</td>
<td>40</td>
<td>177</td>
<td>223</td>
<td>265</td>
<td>303</td>
<td>277</td>
<td>1748</td>
<td>2866</td>
</tr>
<tr>
<td>Spamming</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>305</td>
<td>285</td>
<td>181</td>
<td>2480</td>
<td>8150</td>
</tr>
<tr>
<td>Other Offences related with cyber crimes</td>
<td>4</td>
<td>18</td>
<td>17</td>
<td>264</td>
<td>148</td>
<td>160</td>
<td>188</td>
<td>1240</td>
<td>2417</td>
</tr>
</tbody>
</table>

Graph 3.1-Cyber crime incidents against e-banking

OBSERVATION ON CYBER CRIME INCIDENTS:- Total 23 incidents of cyber crime attacks were reported during the year 2004. During 2005, there was a growth of 231 incidents over the previous year and reported 254 incidents. During the year 2006 there was an absolute growth of 298 incidents as compared to previous year and reported

364 Source- Annual Report of Asia Pacific Computer Emergency Response Team (2012)
365 Ibid
552 incidents. In the year 2007, there was again rise of 685 incidents over the previous year and total 1237 incidents were reported. During the year 2008, total 2565 incidents were reported and there was a rise of 1328 incidents over the previous year. Similarly, in the year 2009, there was again a rise of 5701 incidents and over the previous year and reported 8266 incidents. Likewise, during the year 2010, total 10315 incidents were reported and there was rise of 2049 incidents over the previous year. In the same manner during the year 2011, total 13301 incidents were reported and there was again a rise of 2986 incidents over the previous year while during the year 2012, there was again a rise of 8795 incidents over the previous year and reported 22060 incidents.

It is observed from the above data that from 2004 to 2012 there was a steep rise in the incidents of cyber crime and reported 22037 incidents. The above data depicts that as on 31/03/2012 total incidents of cyber attacks were 13301 which comprises of 4% incidents of phishing, 13% incidents of network scanning/probing, 14% incidents of spreading virus and malicious code, 37% incidents of spam, 21% of website compromise and malware propagation and 11% incidents of other cyber attacks including hacking, carding data theft etc.

It is observed from the above that the cyber regulations and supporting regulations related e-banking operation in India are not adequate and sufficient to control the mounting cyber crime. Therefore the number of incidents has shown the rising trend during last 9 years i.e. from 2004 to 2009 in the cyber crime incidents. Due to mounting of cyber crime incidents it creates the problem for the banking industry. There are the loopholes in the existing statute and it gives the benefits to the miscreants to escape from the punishment. Therefore, it reveals that mounting incidents are creating the problems for e-banking in India. The tremendous rise of cyber crime incidents is due to the problem of law. Therefore it gives the impression that there is no adequate and sufficient legal control of cyber crimes against e-banking in India.

Let us discuss the cyber-crimes generally committed against e-banking in the light of cyber crime incidents handled by Indian Computer Emergency Response Team (CERTIn) as under:
3.4.3(A) PROBLEM OF MOUNTING CYBER CRIME CASES RELATED TO SPREADING VIRUSES, WORMS AND TROJAN HORSE

Spreading Viruses, Worms and Trojan horse: - In maximum incidents, viruses and worms can damage the computers up to any extent as per the intention of the creator of the viruses and worms. The viruses and worms can send the data stored in the computers to anybody else and then delete it. Viruses and worms can hang and disorder the targeted computers and can make them obsolete devoid of a restitution of the operating system. Previously the damage caused to the targeted computers was limited but now a days the damage caused to the computers and data is enormous. Therefore it is a significant threat to banks in terms of resources lost.

Trojan horse: - Trojan horse provides the perpetrator the potential ability to steal passwords and IDs, especially for online banking. Bugbear is a mass-mailing worm and can be used in the same manner to retrieve user names and passwords for online financial accounts.

YEARWISE INCIDENTS OF VIRUSES & MALICIOUS CODE IN INDIA DURING 2004-2012

<table>
<thead>
<tr>
<th>Year</th>
<th>Incidents</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Cyber Security Incidents</td>
<td>23</td>
<td>254</td>
<td>552</td>
<td>1237</td>
<td>2565</td>
<td>8266</td>
<td>10315</td>
<td>13301</td>
<td>22060</td>
<td></td>
</tr>
<tr>
<td>Virus and Malicious Code</td>
<td>5</td>
<td>95</td>
<td>19</td>
<td>358</td>
<td>408</td>
<td>596</td>
<td>2817</td>
<td>2765</td>
<td>3149</td>
<td></td>
</tr>
</tbody>
</table>

A) Observations on the mounting cyber crime cases related to Spreading Viruses, Worms and Trojan Horse.- As per Table No.4, the reported incidents of virus and malicious code were 14 % as compared to total cyber security incidents reported during 2012. There was total rise of incidents of virus and malicious code from 2004 to 2012 to the tune of 3144 and it reveals worrying trend. There is a tremendous rise of cyber crime incidents of spreading viruses, worms and trojan horse from 5 incidents in 2004 to 3149 incidents in 2012 as handled by CERTIn.

B) LEGAL REMEDY AVAILABLE FOR SPREADING VIRUSES, WORMS AND TROJANS IN INDIA

Legal remedy is available under Information Technology (Amendment) Act, 2008, Section 43(c) & 43(e) read with Section 66 and under Section 268 of Indian Penal Code, 1860. Spreading of Virus offence is cognizable offence with boilable and compoundable with a permission of the court before which the prosecution of such offence is pending. It can be trialed before any magistrate.

Data published by CERT In (Computer Emergency Response Team India) in this regards reflects that there is a tremendous rise of crime incidents within a span of nine years since 2004 to 2012 under this category. Therefore it gives the impression that there is no adequate and sufficient legal control of cyber crimes like spreading viruses and worms against e-banking in India. However the IT Act appears sufficient in all respect but it is not competent enough to tackle the problems of such crimes because there are loopholes in the IT Act 2000 and other legislations and the criminals escape easily by taking the advantage of these loopholes. On the basis of the above our interpretation is that the existing cyber laws are inadequate and insufficient to control the cyber crimes against e-banking in India as there is a massive growth in cyber crime incidents.

C) INCIDENTS OF ATTACKS OF VIRUSES, WORMS & TROJANS ON INDIAN BANKING INDUSTRY

I) OTP (ONE TIME PASS WORD) ATTACK USING AN ANDROID MOBILE BOTNET

Major Indian banks such as ICICI, SBI, PNB, HDFC, HSBC etc were targeted for stealing of 2 factor authentications and OTP (One Time Pass Word) attack using an android mobile botnet called “Perkele” which means devil in Finnish.

While doing study on this botnet it was found that there were targets loaded for major Indian bank websites, such as

1) icicibank.com
2) onlinesbi.com
3) pnbindia.in
4) canarabank.in

367 ON 6th of March 2013, Brian Krebs blogged about this malware botnet on loose on Google play store.
II) VIRUS ATTACK ON HSBC TRANSACTIONS WITH OTP DEVICE

The virus attacks two other banks during last year i.e. 2012. The latest one is on HSBC Online banking using a similar Man-in-Middle / Man-in-Browser attack method. It is an attempt to bring to the notice that what an attack can do to an online banking customer using HSBC online banking facility with OTP (One Time Password) Device and how it can result in a similar financial loss. This is a case where a virus can take control of internet explorer and manipulate HSBC Bank transactions in real-time. The user logs into HSBC online bank with the help of One time Password (OTP) (Hardware Device is provided to each user by HSBC Bank) and performs an online transactions. The user should provide a One Time Password (OTP) (OTP is Generated by hardware token every one minute) to confirm any kind of online transaction. The user is unaware that a virus is running in the background. In spite of the dual authentication, the virus is able to manipulate the transaction in real-time without the user’s knowledge and redirects the fund to the attacker’s account.

User account name: Naveen T.G in HSBC Bank with OTP Device
Destination account name: Yash K.S in ICICI Bank
Attacker’s account name: Yash K.S in Citibank

1) User login & Transact: User logsins as Naveen T.G (HSBC Bank), with login password and One Time Password (OTP) into HSBC Bank. User enters the details of destination account information along with the amount of Rs. 34 and confirms the transaction by entering One Time Password (OTP) and completes the transaction.

2) User Realization: The user checks the account statement of HSBC Bank, the user sees that Rs. 10,000 has been transferred instead of Rs. 34 and also, instead of transferring it to Yash K.S – ICICI Bank account, the virus has transferred the amount to Yash K.S – Citibank account in real-time.

[^368]: http://www.ksyash.com/tag/hsbc-bank-attack/
3) **Verification of the Attacker’s account**: This also shows the attacker’s account i.e Yash K.S – Citibank account where the money has been transferred confirming that the virus has been successful in diverting transactions

**III) FIRST EVER CASE OF MOBILE TROJAN SPREADING VIA ‘ALIEN’ BOTNET**

For the first time in the history of mobile cybercrime, a Trojan is being spread using botnet controlled by other criminal groups. It also became clear that Obad.a is mostly found in CIS countries. In total, 83% of attempted infections were recorded in Russia, while it was also detected on mobile devices in Ukraine, Belarus, Uzbekistan and Kazakhstan. Apart from using mobile botnet, this highly complex Trojan is also distributed by spam messages. This is a major carrier of the Obad.a Trojan. Typically a message warning the user of unpaid ‘debts’ lures victims to follow a link which automatically downloads Obad.a onto the mobile device. Again, though, users must run the downloaded file in order to install the Trojan.

**D) LEGAL CASES RELATED TO OFFENCES OF SPREADING VIRUSES, WORMS AND TROJANS HORSE ATTACK**

1) **The US Federal Trade Commission Vs Internet marketing organizations 2006**

In this case “The US Federal Trade Commission” has sued Internet marketing organizations under the “unfairness doctrine” to make them stop infecting consumers’ PCs with spyware. In one case, that against Seismic Entertainment Productions, the FTC accused the defendants of developing a program that seized control of PCs nationwide, infected them with spyware and other malicious software, bombarded them with a barrage of pop-up advertising for Seismic clients, exposed the PCs to security risks, and caused them to malfunction. Seismic then offered to sell the victims an “antispyware” program to fix the computers, and stop the pop ups and other problems that Seismic had caused. On November 21, 2006, a settlement was entered in federal court under which a $1.75 million judgment was imposed in one case and $1.86 million in another, but the defendants were insolvent.

---


In this case, brought against Cyber Spy Software LLC, the FTC charged that Cyber Spy marketed and sold "Remote Spy" key logger spyware to clients who would then secretly monitor unsuspecting consumers’ computers. According to the FTC, Cyber spy touted Remote spy as a “100% undetectable” way to “Spy on anyone from anywhere.” The FTC has obtained a temporary order prohibiting the defendants from selling the software and disconnecting from the Internet any of their servers that collect, store, or provide access to information that this software has gathered. The case is still in its preliminary stages. A complaint filed by the Electronic Privacy Information Centre(EPIC) brought the Remote Spy software to the FTC’s attention.371

3) United States v. Morris (1991) 504, F 2d the U S Court of Appeals for the Second Circuit, 928372

In this case, the accused, released into the internet, a national computer network, a computer programme known as ‘Worm’ which differs from ‘Virus’ and it caused ‘Crash’ and ‘Ceased functioning’ of computers at various educational institutions and military websites. The Northern District Court convicted him under Title 18 USC Section 1030 (a) 5 (A). Morris then preferred an appeal before the Circuit Court. The Circuit Court concluded that Section 1030 (a) 5 (A) does not require the Government to demonstrate that the defendant intentionally prevented authorized use and thereby caused loss. There was sufficient evidence for the jury to conclude that Morris acted ‘without authorization’ within the meaning of Section 1030 (a) 5 (A). Morris was sentenced to 3 years of probation, community service for 400 hours and a fine of $ 10,050.

4) The trail of Masato Nakatsuji on Trojan Horse case in the Court in Kyoto of Japan 2008373

In this case, a person admits in court to write anime Trojan horse that attacked P2P users. Experts at Sophos Labs. Sophos's global network of virus, spyware and spam analysis centers, have reminded businesses of the importance of protecting their

372 http://cyberlaw.com/cyberlaw cases as summarized by Roy August
networks from virus attack, as a Japanese man admits in court to writing a data-
destroying Trojan horse. 24-year-old Masato Nakatsuji, who was revealed to be the first
ever virus writer to be arrested in Japan when he was apprehended in January 2008,
admitted in Kyoto District Court that he created a Trojan horse and used copyrighted
animation footage to spread it via the net. Nakatsuji has admitted to having written the
malware which displayed images of popular anime characters while wiping music and
movie files from users’ computers. The malicious code, believed to be the Pirlames
Trojan, was spread via the controversial Winny file-sharing system in Japan last year.
Nakatsuji made the admission during the first day of the trial, where he answered
charges of copyright infringement and defaming an acquaintance by embedding his
photograph into the malicious code. The court in Kyoto heard prosecutors describe how
Nakatsuji is alleged to have created the Trojan horse, attached it to copyrighted
animated pictures and planted links to it on internet message forums. However,
Nakatsuji’s defense team has argued that the malware was not seriously malignant, and
that justice would not be served by punishing the graduate student of Osaka Electro-
Communication University for spreading the Trojan horse when there were no specific
laws against it

916

In the present case Hon’ble Supreme Court articulated that simply entered into the
property of the other person without motive is not the criminal tress pass. To established
the criminal tress pass in the others property the criminal must have a apparent motive
and adequate knowledge of to commit crime. But when a cyber criminal intrude into the
computer systems of the other person without his knowledge and permission to commit
further crime. The criminals unauthorized access information which may be exploited by
him or not; he will be punished u/s 66 of the Information Technology Act, 2000. The
Information Technology Act 2000 has a provision for search and seizure of the computer
and other storage devices out of the possession of the cyber criminal because the data
or information is so valuable and delicate that only access may diminish its importance.

374 AIR 1964 SC 986; (1964) 5 SCR 916; (1964) 2 Cr LJ 57
3.4.3(B) PROBLEM OF MOUNTING OFFENCES OF WEBSITE COMPROMISE & MALWARE PROPAGATION INCLUDING DENIAL OF SERVICE (DoS) AND DISTRIBUTED DENIAL OF SERVICE (DDoS) IN INDIA

Website Compromise and Malware Propagation:- Website Compromise is often referred to as phishing. It involves the aggressor bringing into light, or exposing, information about the victim. Website Compromise is simply the act of bringing into light information that is private or sensitive in nature. Often obtained directly from the victim without their knowledge or by using readily available information about the victim to extract further information. Malware or malicious software is used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware is often used against individuals to gain personal information such as social security numbers, bank or credit card numbers, and so on.

Denial of Service (DoS)/ Distributed Denial of Service (DDoS):- A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

YEAR-WISE INCIDENTS OF WEBSITE COMPROMISE & MALWARE PROPAGATION INCLUDING DENIAL OF SERVICE (DoS) & DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACK IN INDIA DURING 2004-2012

Table 3.17- Incidents of Website Compromise & Malware Propagation in India during 2004-2012

<table>
<thead>
<tr>
<th>Year</th>
<th>Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Cyber Security Incidents</td>
<td>23</td>
</tr>
<tr>
<td>Website Compromise and Malware Propogration</td>
<td>-</td>
</tr>
</tbody>
</table>

Source: - Annual Report of Asia Pacific Computer Emergency Response Team (2004-12)
A) Observations on the mounting offences of Website Compromise and Malware propagation including Denial of Service (DoS)/ Distributed Denial of Service (DDoS):- As per Table No.5, the reported incidents of Website Compromise and Malware propagation including Denial of Service(DoS)/ Distributed Denial of Service (DDoS) reported incidents were 21 % as compared to total cyber security incidents reported during 2012. The total rise of incidents of Website Compromise & Malware Propagation from 2008 to 2012 was 3756 incidents depicting the serious concern over the situation. There is a tremendous rise of cyber crime incidents of Website Compromise & Malware Propagation from 835 incidents in 2008 to 4591 incidents in 2012 as handled by CERTIn.

B) LEGAL REMEDY AVAILABLE FOR WEBSITE COMPROMISE & MALWARE PROPAGATION IN INDIA

In India there is no law, which is specifically dealing with prevention of malware through aggressive defense. Thus, the analogous provisions have to be applied in a purposive manner. The protection against malware attacks can be claimed under the following categories:

(1) Protection available under the Constitution of India,
(a) Article 19(1) (g),(b) Article 21, (c) Article 300A, and (d) Articles 301 to 305.
(2) Protection available under other statutes.
(A) (A) Protection under I.P.C: (i) Section 22, 23,29, 29A read with Section 2(1) (t) of the IT Act, 2000, Section 32, 33 40,43, 44,96,97,99,268,378 and Section 425
Legal remedy is available under Information Technology (Amendment) Act, 2008, Section 43(c) & 43(e) read with Section 66 and under Section 268 of Indian Penal Code, 1860. Section 65 & 66 are dealt with the offences related with Website Compromise & Malware propagation. The offences are cognizable offences with bailable and compoundable with a permission of the court before which the prosecution of such offence is pending. Section 43 addresses the civil offence of theft of data. Concealing, destroying, and altering any computer source code when the same is required to be kept or maintained by law is an offence punishable with three years imprisonment or two lakh rupees or with both Criminalities in the offence of data theft is being separately dealt with later under Sections 65 and 66.
Data published by CERT-IN (Computer Emergency Response Team India) in this regards reflects that there is a tremendous rise of crime incidents within a span of nine years since 2004 to 2012 under this category. Therefore it gives the impression that there is no adequate and sufficient legal control of cyber crimes like Website Compromise and Malware Propagation against e-banking in India. However the IT Act appears sufficient in all respect but it is not competent enough to tackle the problems of such crimes because there are loopholes in the IT Act 2000 and other legislations and the criminals escape easily by taking the advantage of these loopholes. On the basis of the above our interpretation is that the existing cyber laws are inadequate and insufficient to control the cyber crimes against e-banking in India as there is a massive growth in cyber crime incidents.

C) INCIDENTS OF ATTACK OF MALWARE PROPAGATION ON INDIAN BANKING INDUSTRY

1) MALWARE THAT DEMANDS $300 TO RELEASE YOUR DATA\textsuperscript{376}

Mint Mumbai has published the news on web that a malware that goes by the name ‘Crypto locker’ has been encrypting or locking data files of gullible users who inadvertently install it, and demands a ransom of $300 to release the data. Other malware of this nature, commonly clubbed as Ransomware, can be tackled using a decent anti-virus program as a recovery tool. But “Crypto locker” is very different. The incidents are being reported from all over India. It is essential that everyone connected to the Internet is aware of such a damaging malware.

Ransomware spreads using social engineering tricks especially via email such as fake FedEx or UPS tracking notifications with attachments. Once the victim opens such email attachments, Crypto locker gets installed and starts scanning the hard disk for all kinds of documents. Quick Heal Threat Research and Response Lab said it received reports of several incidents involving this malware, including from users in India, that once executed encrypts files in the victim’s computer and demands a certain ransom for decryption. This malware makes demand of $300 through prepaid card services such as UKash, Bitcoin or MoneyPak, said Quick Heal in a release. These include images,

\textsuperscript{376} http://www.livemint.com the news on Wall Street Journal
videos, documents, presentations and spreadsheets. Thereafter, it encrypts these files, converting them into an unreadable form. The Ransomware then pops up a message, in which it demands the victim pay up $300 (currently) to buy a private key to decrypt the files.

Crypto locker uses unique an encryption method of public private key pair to encrypt each of its victim’s data. Since the decryption key is not stored on the infected computer, it is very difficult to decrypt the data encrypted by this malware, note anti-virus experts. The malware gives a deadline of 100 hours to pay the ransom and get the private key to decrypt the data. If the amount is not paid, it destroys the private key and your encrypted data is locked forever with no way to recover it. Hackers behind this malware are able to avoid the trace back by using digital cash systems such as Bitcoins and Money Pack where the payments can be anonymous. Online security firm Sophos identified Crypto locker as “Troj/Ransom-ACP” a spyware malware.

2) GLOBAL CREDIT CARD FRAUD: NEW MALWARE BEHIND FRAUD, SUSPECT BANKERS

Mayur Shetty, in his article published in Times of India | Feb 7, 2013 said that Bankers say that the explode in credit card frauds is possibly caused by a new malware “Dexter” which has been used to commit digital fraud internationally."Dexter" is malware, which is of recent origin is termed by payment industry experts as a highly intelligent one as it directly communicates with the command-and-control server and instructs the systems to grab and transmit any credit card data that comes into the machine. The malware uses the retailer’s network which is typically not secured since they are used for non-critical data.

Use of malware in digital fraud has made it difficult for authorities to nab the fraudsters even when there is coordinated international effort. This is because the hacker who receives the information from the Malware does not use it himself but sells it anonymously over the net to buyers across the world. Scamsters buy individual information after sampling few card numbers. Bankers say that since cards are invariably blocked after an initial transaction, scamsters buy card information in bulk and

---

these are sold at prices as low as $2 per card information. Once this information is available it can be used to clone cards. Theoretically, card information can be stolen from a retail chain in India, by a hacker in Russia and sold to scamsters in United States.

While RBI has done its best to make transactions secure it cannot prevent international frauds. Since most of the cards issued by Master Card and Visa are international cards they can be freely used outside the country. The card information can also be used in online transactions because in some countries there are e-commerce sites that conclude a transaction without even the CVV2 number which is printed on the reverse of the credit card. (CVV2 is an important security feature for credit card transactions on the Internet and over the phone. "CVV" stands for "Card Verification Value")

3) ATTACKERS TURN BANK OF INDIA SITE INTO MALWARE BAZAAR

Bank of India IT staff is mopping up the mess left by attackers who rigged the firm’s website to feed malware to customers trying to access online services. The bank managed to pry loose the rogue i-frame responsible for the malware sometime early Friday morning California time. At time of writing, though, Bank of India’s website was effectively cordoned off, bearing a terse notification saying: "This site is under temporary maintenance and will be available after 09:00 IST on 1.09.07." The shutting came a day after employees for security provider Sunbelt Software discovered someone had planted an iframe in the site that caused un patched Windows machines to be infected with some of the most destructive pieces of malware currently in circulation. Sunbelt counted 31 separate pieces including Pinch, a powerful and easy to use Trojan that siphons personal information from a user’s PC. Other malware included Trojan, Netview, Trojan-Spy, Win32, Agent.ql.various root kits and several spam bots.

Executives and IT administrators at US offices of Bank of India who were contacted Friday morning by IDG were initially unaware of the attack. A spokesman later told the news service that officials were aware of the problem and were working to correct it. But he had no information concerning its severity or duration.

---

379 https://www.google.co.in
Some of the servers used to install the malware belonged to the notorious Russian Business Network, a group Spamhaus says is involved in child porn, phishing and other misdeeds. According to Verisign’s iDefence unit, The RBN also played a hand in bringing usMPack, a powerful Trojan downloader that infect Edmore than 10,000 websites in just three days.

Roger Thomson, a researcher with Exploit Prevention Labs, said he spotted one piece of code that exploited a vulnerability patched by last year’s Microsoft Security Bulletin MS06-042. “It’s pretty much a cut-and-paste of the original proof-of-concept that was put out on last July” Thomson said of the code

The Web site of Bank of India, one of India’s leading banks, was restored early Tuesday. The bank had closed the site on Friday after it found that the site had been hacked, and was dispensing malicious code. Sunbelt Software Inc. a provider of security software in Clearwater, Fla., had on Thursday alerted users on its blog that the bank’s site had been compromised, and advised them not to visit the site. Unidentified hackers had inserted malicious code into the bank’s main Web page, a senior employee familiar with the situation said on Tuesday, speaking on condition of anonymity. The bank's designated spokesman on this issue was not immediately available for comment. As a result, persons coming to the bank's Web site were likely to be temporarily redirected to another site where Trojans and other malware were downloaded onto their computers, the employee said. The user was then brought back to the bank Web site. The bank's IT staff thought they had the situation under control Friday morning, until they found that each time they changed the index page for the Web site, it was immediately replaced by the hackers. The bank then decided to bring the Web site down.

The bank has since changed the company hosting the service. The attack on the Web site did not, however, affect the bank's online banking operations, according to the employee. The bank's customers access online banking services through a link on the home page of the bank's Web site. The online banking service is provided to users from well-protected servers hosted and monitored within the bank by Hewlett-Packard Co., the employee said.
The bank is as yet not clear about the identity of the hackers, although Sunbelt suggested in its blog that it was a criminal gang, called the Russian Business Network (RBN). "We have called for the logs from the hosting provider in the U.S., and we may have some definite information then," the employee said.

D) LEGAL CASES RELATED TO OFFENCES OF WEBSITE COMPROMISE AND MALWARE ATTACKS

1) ZANGO, INC. (Plaintiff-Appellant), Vs KASPERSKY LAB, INC., (Defendant-Appellee ). No. 07-35800 D.C. No. CV-07-00807-JCC OPINION

In this case the U.S. District Court ruled against an online media company that wanted to force Kaspersky Lab to stop classifying its adware as "spyware."

Facts of the case:- Zango, an online media company, came up short in its attempt to force an anti-virus company to reclassify its "spyware" tag for the company's adware. The U.S. District Court for the Western District of Washington ruled in favor of Kaspersky Lab, granting the security company immunity from liability in a suit filed by Zango. According to Kaspersky, Zango sued them to force the company to reclassify Zango's programs as "non-threatening" and to prevent Kaspersky's security software from blocking Zango's programs.

"Kaspersky Lab's mission is, and has always been, to make the Internet a safer place for all," said Steve Orenberg, president of Kaspersky Lab, USA, in a statement. "We are thrilled with the outcome of this case because it supports the key message of the information security industry -- consumer protection comes first."

The judge threw out Zango's lawsuit on the grounds that Kaspersky was immune from liability under the Communications Decency Act, part of which states that a provider or user of an interactive computer service shall not be held liable on account of any action voluntarily taken in good faith to restrict access to material that the provider or user considers to be "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." Kaspersky noted that the ruling protects the consumer's right to determine what information and software is allowed on their computer, and gives anti-malware vendors the right to identify and label software programs that may be potentially unwanted and harmful to a user's computer as they see fit.

2) VBS/LOVELETTER AND LOVE BUG WORM.\textsuperscript{382}

Facts of the case:- It began in Philippines on 4th May 2000 and spread over the world in one day through email boxes. It infected 10\% of all computers connected to the internet. Only Microsoft windows operating system effected. Subject line: “ILOVEYOU”. Attachment LOVE-LETTER-FOR-YOU.TXT.vbs. Damage about Rs. 22,000 Crore. The Pentagon, British Parliament and most of the corporation shut down the email systems to get rid of this worm.

Affecting the worm search all drives which are connected to the infected computer and replace files. The worm propagates by sending out copies of itself to all entries in the Microsoft Outlook address book.

Action: There was no law against virus writing in Philippines; hence prosecutors dropped all the charges against the offender. Govt. of Philippines enacted a Philippines Commerce Law on 14th June 2000 to deal with Cyber Crime.

3) State of Chhattisgarh vs Prakash Yadav & Manoj Singhania\textsuperscript{383}

Mr. Manoj Singhania, head of the local branch of Aptech and another Prakash Yadav, in-charge of training institute were tried to hack into the computers of the State Bank of India Raigarh Branch. Clearly a case of Spyware and Malware The duo were arrested for sending e-mails in the name of Microsoft and Videsh Sancher Nigam Ltd. (VSNL) India containing programme file named ‘Speed.exe.’ As soon as the file was opened it automatically sent to accuse the password, data and other information of the user.

4) Sony BMG Vs Girard Gibbs and Kamber & Associates New York CD Technologies Litigation, Case No. 1:05-09676-NRB.\textsuperscript{384}

Sony BMG has rushed forth to settle a class action lawsuit brought by Girard Gibbs and Kamber & Associates in New York over its embarrassing rootkit scandal. A few months ago it came to light that Sony was using a particularly egregious form of copy protection on CDs that implants hooks into the Windows kernel to make sure you don't use the CD in a manner of which Sony doesn't approve. The so-called rootkit caused a furor online and in the media, and after trying to play it down as par for the course, Sony eventually

\textsuperscript{382} en.wikipedia.org/wiki/ILOVEYOU
\textsuperscript{383} http://www.landfield.com/lsn/mail-archive/2001/Jan/0139.html
relented and claimed it would no longer use the DRM in question. That didn't stop the lawsuits, however. A class action lawsuit was filed in California within days of the evidence becoming public, and suits in other regions followed quickly.

The settlement will include a promise by Sony to stop all use of the XCP and MediaMax DRM technologies, which is a given. Then, after paying lawyers' fees (what is a class action for, if not that?), the company will recall all remaining XCP and MediaMax DRM-backed CDs, and then compensate customers who have purchased the ill-begotten discs. Sony has said that it was recalling discs previously, but the company says it is having trouble getting all retailers to comply.

Customers who purchased the poisoned discs will have two options. First, they can cash in on a payment of US$7.50 per CD they purchased (aka, much less than they paid for it), and snag one free album download. Or, if one don't want to bother with cashing a check for $7.50, the cash payment can be cast aside in favor of three free album downloads. In both instances, the offending CDs will be replaced with DRM-free discs, but the album downloads will most likely use a less heinous form of DRM. The company will also be required to provide a safe tool for removing the root kits.

Perhaps the most interesting aspect of this settlement is the requirement regarding downloadable albums. Sony has the right to limit the albums that are available to a list of 200, but the company cannot force you to use their music store. Instead, Sony must use at least three different venues to distribute content: Settlement Class Members may download albums from any one of three major download services. SONY BMG will use commercially reasonable efforts to offer Apple Computer, Inc.’s popular iTunes as one of the download services available to Settlement Class Members. The settlement will not take place until it is approved by the court. Proof of purchase will be required, or proof of a return if a disc was taken back to a retailer after November 14.

Will this be enough to restore Sony's reputation? It depends on who you ask. The general public has probably forgotten about Sony already, but the technology community will remember this for a very, very long time. Let's hope that the public shame of a class action serves as a warning to other companies who are willing to endanger our personal property for no good reason whatsoever.
5) Yehuda Michaekli, on behalf of himself and all other similarly situated (Plaintiff) Vs eXact Advertising (Defendant), CIV No. 05 CV8331 in United States District Court Southern District of New York, Sep. 27, 2005

Summary: lawsuit filed against adware company eXact Advertising on September 27, 2005 by law firm Shalov Stone & Bonner LLP in US District Court Southern District of New York. The suit was filed on behalf of plaintiff Yehuda Michaekli as a class action complaint with jury trial demanded. eXact has unlawfully used and damaged Plaintiff's rights to use and enjoy his personal property. Without Plaintiff's authorization, eXact Advertising infected Plaintiff's computer with harmful and offensive spyware programs by deceptively bundling its malicious software with "free" games, cursors, screensavers and other small software programs. These harmful programs would then secretly track Plaintiff's Internet use, thereby invading his privacy and damaging his computer. In addition to invading Plaintiff's privacy, eXact Advertising's unwanted spyware and adware programs illicitly caused Plaintiff's computer to slow down, consume excessive bandwidth monopolize computer resources including memory, pixels and monitor space, and disable or destroy user installed computer software ultimately causing many computers to crash."


In 2010, Webcam Gate Case, plaintiffs charged two suburban Philadelphia high schools secretly spied on students by surreptitiously and remotely activating webcams embedded in school-issued laptops the students were using at home, and therefore infringed on their privacy rights. The school loaded each student's computer with LANrev remote activation tracking software. This included the now-discontinued "Theft Track". While Theft Track was not enabled by default on the software, the program allowed the school district to elect to activate it, and to choose which of the Theft Track surveillance options the school wanted to enable.

386 http://www.whitman.edu/rhetoric/decisions/12-drew-nicholas-robbins-webcam.htm
Theft Track allowed school district employees to secretly remotely activate a tiny webcam embedded in the student’s laptop, above the laptop’s screen. That allowed school officials to secretly take photos through the webcam, of whatever was in front of it and in its line of sight, and send the photos to the school’s server. The LANrev software disabled the webcams for all other uses (e.g., students were unable to use Photo Booth or video chat), so most students mistakenly believed their webcams did not work at all. In addition to webcam surveillance, Theft Track allowed school officials to take screenshots, and send them to the school’s server. In addition, LANrev allowed school officials to take snapshots of instant messages, web browsing, music playlists, and written compositions. The schools admitted to secretly snapping over 66,000 web shots and screen shots, including webcam shots of students in their bedrooms.

7) State of New York v. Intermix Media, 2005 WL 1034041 (verified petition filed April 28, 2005)\(^{387}\).

In this case suit brought In 2005 By Spitzer, The California Firm Intermix Media. Inc, ended up settling, by agreeing to pay Us$7.5 Million and to stop distributing spyware\(^{388}\).

**Facts of the case:** Former New York State Attorney General and former Governor of New York Eliot Spitzer has pursued spyware companies for fraudulent installation of software. In a suit brought in 2005 by Spitzer, the California firm Intermix Media, Inc. ended up settling, by agreeing to pay US$7.5 million and to stop distributing spyware. The hijacking of Web advertisements has also led to litigation. In June 2002, a number of large Web publishers sued Claria for replacing advertisements, but settled out of court.

Courts have not yet had to decide whether advertisers can be held liable for spyware that displays their ads. In many cases, the companies whose advertisements appear in spyware pop-ups do not directly do business with the spyware firm. Rather, they have contracted with an advertising agency, which in turn contracts with an online subcontractor who gets paid by the number of "impressions" or appearances of the

\(^{387}\) http://itlaw.wikia.com/wiki/New_York_v._Intermix_Media
\(^{388}\) http://en.wikipedia.org/wiki/Spyware
advertisement. Some major firms such as Dell Computer and Mercedes-Benz have sacked advertising agencies that have run their ads in spyware.

8) Syed Asifuddin & Ors. Vs State of Andhra Pradesh & another - 2005 CrLJ 4314 (AP)

These two petitions are filed by different persons under section 482 of Code of Criminal Procedure, 1973 (Cr. P.C.) seeking similar relief. Both the matters were admitted on the same day and since then both the matters are being disposed of as such, this common order covers both the matters. The petitioners in both the matters seek the relief of quashing FIR No. 20 of 2003 of Criminal Investigation Department (CID) Police, Hyderabad, registered under section 409, 420 and 120B of Indian Penal Code, 1860 (for short, IPC), Section 65 of the Information Technology Act, 2000 (for short IT Act) and section 63 of the copyright Act, 1957 (for short, Copyright Act).

While admitting the petition, this Court passed orders in criminal miscellaneous petition No. 3951 of 2003 staying all further proceeding including investigation of the crime pending disposal of the main petition. The Public Prosecutor filed criminal miscellaneous petition No. 232 of 2005 for vacating the said order. The matter was "Finally heard at that stage itself and are being, disposed of finally. The main allegation against the petitioners is that the MIN of Reliance phone is irreversibly integrated with ESN and the petitioners hacked ESN so as to wean away RIM customer to TATA Indicom service. The question is whether the manipulation of this electronic 32-bit number (ESN) programmed into Samsung N191 and LG-2030 cell phone instrument exclusively franchised to second respondent amounts to altering source code used by these computer handsets i.e., cell phone instruments. In the background facts, a question would also arise whether such alteration amounts to hacking with computer system? If the query answered in the affirmative, it is always open to the police to alter the FIR or it is always open to the criminal Court to frame a charge specifically with regard to hacking with computer system, which is an offence under Section 66 of the IT Act. At this stage, we may read Sections 65 and 66 of the IT Act.

Crime No. 20 of 2003 in so far as it is under section 409, 420 and 120B of Indian Penal Code, 1860 is quashed and insofar as the crimes under Section 63 of the Copyright Act, 1957, the criminal petitions are dismissed. The CID Police, which registered Crime No. 20
of 2003, is directed to complete investigation and file a final report before the Metropolitan Magistrate competent to take cognizance of the case within a period of Three months from the date of receipt of this order. The criminal petitions are accordingly dismissed

3.4.3(C) PROBLEM OF MOUNTING CASES RELATED TO PHISHING OFFENCES

Phishing/ Vishing attack: - Phishing scams are designed to attract the user to provide the card number and PIN for their bank card. The information is collected by the thieves and used to create fraudulent cards

YEARWISE INCIDENTS OF PHISHING IN INDIA DURING 2004-2012

<table>
<thead>
<tr>
<th>Year</th>
<th>Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>23</td>
</tr>
<tr>
<td>2005</td>
<td>254</td>
</tr>
<tr>
<td>2006</td>
<td>552</td>
</tr>
<tr>
<td>2007</td>
<td>1237</td>
</tr>
<tr>
<td>2008</td>
<td>2565</td>
</tr>
<tr>
<td>2009</td>
<td>8266</td>
</tr>
<tr>
<td>2010</td>
<td>10315</td>
</tr>
<tr>
<td>2011</td>
<td>13301</td>
</tr>
<tr>
<td>2012</td>
<td>22060</td>
</tr>
</tbody>
</table>

A) Observations on the mounting cyber crime cases related to Phishing offences: - As per Table No.6, the reported incidents of phishing were 4 % as compared to total cyber security incidents reported during 2012. There was total rise of incidents of phishing from 2004 to 2012 to the tune of 884 and it reveals worrying trend. There is a tremendous rise of cyber crime incidents of phishing scam from 3 incidents in 2004 to 887 incidents in 2012 as handled by CERTIn.

B) LEGAL REMEDY AVAILABLE FOR OFFENCES OF PHISHING

The provisions of Information Technology Act, 2000

The phishing fraud is an online fraud in which the fraudster disguise themselves and use false and fraudulent websites of bank and other financial institutions, URL Links to deceive people into disclosing valuable personal data, later on which is used to swindle money from victim account. Thus, essentially it is a cyber crime and it attracts many penal provisions of the Information Technology Act, 2000 as amended in 2008 adding

390 Source: - Annual Report of Asia Pacific Computer Emergency Response Team (2004-12)
some new provisions to deal with the phishing activity. The following Sections of the Information Technology Act, 2000 are applicable to the Phishing Activity:

Section 43: This section makes adequate provision for the aggrieved party to seek compensation (which may be up to Rs. 1 Crore) for unauthorized access to his personal/private data\(^{391}\).

Section 66: The account of the victim is compromised by the phisher which is not possible unless & until the fraudster fraudulently effects some changes by way of deletion or alteration of information/data electronically in the account of the victim residing in the bank server. Thus, this act is squarely covered and punishable u/s 66 IT Act\(^{392}\).

Section 66A: The disguised email containing the fake link of the bank or organization is used to deceive or to mislead the recipient about the origin of such email and thus, it clearly attracts the provisions of Section 66A IT Act, 2000\(^{393}\).

Section 66C: In the phishing email, the fraudster disguises himself as the real banker and uses the unique identifying feature of the bank or organization say Logo, trademark etc. and thus, clearly attracts the provision of Section 66C IT Act, 2000\(^{394}\).

Section 66D: The fraudsters through the use of the phishing email containing the link to the fake website of the bank or organizations personates the Bank or financial institutions to cheat upon the innocent persons, thus the offence under Section 66D too is attracted\(^{395}\).

Section 420 IPC which related to Cheating: Because phishers use false and fraudulent websites, URL Links to deceive people into disclosing valuable personal data, phishing schemes which is used later to swindle money from victim account. Thus, it is an offence of cheating punishable u/s 420 IPC.

Section 120-B IPC which relates to Criminal Conspiracy: There is also criminal conspiracy between various persons perpetrating the crime, like the persons who open the beneficiary account or who receive the funds in their account in conspiracy with the

\(^{391}\) IT ACT 2000 and ITAA2008
\(^{392}\) ibid
\(^{393}\) ibid
\(^{394}\) ibid
\(^{395}\) IT ACT 2000 and ITAA2008
fraudster. Thus, Section 120-B IPC which relates to criminal conspiracy is also applicable.

**Section 468 IPC which relates to Forgery:** - Website which is in the nature of electronic record to cheat the gullible bank customers is punishable u/s 468 IPC.

**Section 471 IPC which relates to Fraud:** - Further fraudulently or dishonestly use as genuine, the fake website in the nature of electronic record is punishable u/s 471 IPC

Data published by CERT-IN (Computer Emergency Response Team India) in this regards reflects that there is a tremendous rise of crime incidents within a span of nine years since 2004 to 2012 under this category. Therefore it gives the impression that there is no adequate and sufficient legal control of cyber crimes like Phishing against e-banking in India. However the IT Act appears sufficient in all respect but it is not competent enough to tackle the problems of such crimes because there are loopholes in the IT Act 2000 and other legislations and the criminals escape easily by taking the advantage of these loopholes. On the basis of the above our interpretation is that the existing cyber laws are inadequate and insufficient to control the cyber crimes against e-banking in India as there is a massive growth in cyber crime incidents.

**C) INCIDENTS OF PHISHING ATTACKS AS FOLLOWS:**

1) **UTI Bank Hooked up in a Phishing attack**
Fraudsters of cyberspace have reared its ugly head, the first of its kind this year, by launching a phishing attack on the website of Ahmadabad-based UTI Bank, a leading private bank promoted by India’s largest financial institution, Unit Trust of India (UTI). A URL on Geocities that is almost a facsimile version of the UTI Bank's home page is reported to be circulating amongst email users. The web page not only asks for the account holder's information such as user and transaction login and passwords, it has also beguilingly put up disclaimer and security hazard statements.

In case you have received any e-mail from an address appearing to be sent by UTIBANK, advising you of any changes made in your personal information, account details or information on your user id and password of your net banking facility, please do not respond. It is UTI Bank's policy not to seek or send such information through email. If you have already disclosed your password please change it immediately, “the
warning says. The tricky link is available on http://br.geocities. If any unsuspecting account holder enters his login id, password, transaction id and password in order to change his details as 'advised' by the bank, the same info is sent vide mailform.cz (the phishers database).

As per the findings of UTI Bank's security department, the phishers have sent more than 1,00,000 emails to account holders of UTI Bank as well as other banks. Though the company has kicked off damage control initiatives, none of the initiatives are cent percent foolproof. 

The bank has sent alerts to all its customers informing about such malicious websites, besides beefing up their alert and fraud response system. "Engaging professional companies like Fraud Watch help in reducing time to respond to attacks," said Sanjay Haswar, Assistant Vice President, Network and Security, UTI Bank.

2) Phishing attack related to ICC World Cup 2011

The most awaited tournament for cricket lovers, the ICC World Cup 2011, begins on February 19, 2011 was also under phishing attacks. The ICC World Cup is being played in the Indian subcontinent, and the country's cricket-crazy population is all set to get hold of World Cup tickets in every possible way—all to witness and experience live international cricket in action. Since this is a hugely followed international sporting event across the world, Symantec has anticipated spam attacks and other Internet threats related to the event. As expected, we are observing World Cup spam in the Symantec Probe Network.

3) State Bank of India Case

Web sense Security Labs has received reports of a phishing attack that targets customers of State Bank of India. This phishing site is hosted in the United States. The content of the e-mail were as —Dear Valued SBI®Net banking Customer, SBI's Internet Banking, is hereby announcing the New Security Upgrade. We've upgraded our new SSL servers to serve our customers for a better and secure banking service,

---

397 http://www.moneycontrol.com/india/news/pressnews/60-india-inc-believed-to-have-received-phishing-lureswebsense/281565
against any fraudulent activities. Due to this recent upgrade, you are requested to update your account information by following the reference below. (November, 15, 2006). Banking sources indicate that besides SBI, three other international banks have informed CERT-In about attempts at phishing.

D) LEGAL CASES RELATED TO OFFENCES OF PHISHING ATTACKS

1) Umashankar Sivasubramaniam Vs. ICICI Bank (Petition No. 2462/2008 dated 18.04.2010)\(^{398}\)

In a landmark verdict in a phishing case in India, first lawsuit has been registered under the Information Technology Act, against the ICICI Bank. P W C Davidar, Tamil Nadu IT secretary and adjudicator for the state, ordered ICICI Bank on April 12, 2010 to make a compensation of Rs 12.85 Lakh (Rs 1.285 Million) to an NRI customer. The customer complained that he lost this huge amount of money from his bank account as a result of phishing attack in 2007 in Chennai, as per the news published by rediff business on April 12, 2010.

The decision surfaced on an appeal filed by Umashankar Sivasubramaniam. He asserted that he got e-mail in September 2007 from ICICI Bank, according to which, his account would be deactivated if he did not respond with his Internet banking username and password. He responded only to know that Rs 6.46 Lakh were channelized from his bank account to that of a firm, which drew off Rs 4.6 Lakh from the Mumbai branch of ICICI and retained the balance in its account.

The adjudicator continued to accept the plaintiff's statement that the Bank failed to exert due carefulness, and was thus fully liable under Section 85 of the Act, according to which, the Bank had to compensate the victim. He said that the bank was accountable for the loss.

Reportedly, systems and mechanisms of the Bank, prior to and right after the charge of this offence and the lack of KYC liability were also spot lit. However, the main point that is highlighted in the verdict is that ICICI failed to use suitable validation of its e-mails to


275
the consumers in the form of "Digital Signatures". Hence, there was no clue by which
naïve customers could key out an e-mail being sent from ICICI.
In fact, the judge said no effort in this regard was seen from ICICI's side. He further
added in the light of this case, access to the account details of the petitioner, very poorly
mirrors the systems and procedures of the Bank.
Experts, commenting on this issue, said that as there are scores of phishing frauds
taking place in the Indian set-up, this verdict is expected to be welcomed by the huge
population of Indian Internet banking customers.

2) National Association of Software and Service Companies (Nasscom), vs Ajay
In a landmark judgment in the case of National Association of Software and Service
Companies vs Ajay Sood & Others, delivered in March, '05, the Delhi High Court
declared `phishing' on the internet to be an illegal act, entailing an injunction and
recovery of damages.
Elaborating on the concept of 'phishing', in order to lay down a precedent in India, the
court stated that it is a form of internet fraud where a person pretends to be a legitimate
association, such as a bank or an insurance company in order to extract personal data
from a customer such as access codes, passwords, etc. Personal data so collected by
misrepresenting the identity of the legitimate party is commonly used for the collecting
party's advantage. Court also stated, by way of an example, that typical phishing scams
involve persons who pretend to represent online banks and siphon cash from e-banking
accounts after conning consumers into handing over confidential banking details.
The Delhi HC stated that even though there is no specific legislation in India to penalise
phishing, it held phishing to be an illegal act by defining it under Indian law as “a
misrepresentation made in the course of trade leading to confusion as to the source and
origin of the e-mail causing immense harm not only to the consumer but even to the
person whose name, identity or password is misused.” The court held the act of
phishing as passing off and tarnishing the plaintiff's image.

The plaintiff in this case was the National Association of Software and Service
Companies (Nasscom), India's premier software association. The defendants were
operating a placement agency involved in head-hunting and recruitment. In order to obtain personal data, which they could use for purposes of headhunting, the defendants composed and sent e-mails to third parties in the name of Nasscom.

The high court recognised the trademark rights of the plaintiff and passed an ex-parte ad interim injunction restraining the defendants from using the trade name or any other name deceptively similar to Nasscom. The court further restrained the defendants from holding themselves out as being associates or a part of Nasscom. The court appointed a commission to conduct a search at the defendants' premises. Two hard disks of the computers from which the fraudulent e-mails were sent by the defendants to various parties were taken into custody by the local commissioner appointed by the court. The offending e-mails were then downloaded from the hard disks and presented as evidence in court.

During the progress of the case, it became clear that the defendants in whose names the offending e-mails were sent were fictitious identities created by an employee on defendants' instructions, to avoid recognition and legal action. On discovery of this fraudulent act, the fictitious names were deleted from the array of parties as defendants in the case. Subsequently, the defendants admitted their illegal acts and the parties settled the matter through the recording of a compromise in the suit proceedings. According to the terms of compromise, the defendants agreed to pay a sum of Rs1.6 million to the plaintiff as damages for violation of the plaintiff's trademark rights. The court also ordered the hard disks seized from the defendants' premises to be handed over to the plaintiff who would be the owner of the hard disks.

This case achieves clear milestones: It brings the act of “phishing” into the ambit of Indian laws even in the absence of specific legislation; It clears the misconception that there is no “damages culture” in India for violation of IP rights; This case reaffirms IP owners’ faith in the Indian judicial system’s ability and willingness to protect intangible property rights and send a strong message to IP owners that they can do business in India without sacrificing their IP rights.
3) Shri Thomas Raju Vs. The Branch Manager, ICICI Bank, Anna Nagar Branch, Chennai Case decided by- the adjudicating officer, Government of Tamilnadu, Civil Jurisdiction Petition No.3 of 2011 dated 16th May 2011.

Petitioner, an employee of a Chennai based IT company, suffered a loss of Rs. 1,62,800/- as a result of the phishing attack. The said amount was supposed to have been transferred on the account of another customer of ICICI Bank. Petitioner claimed that he had suffered a wrongful loss due to unauthorized access to his savings account of the Anna Nagar branch of ICICI Bank. Petitioner further claimed that he had suffered a loss as bank has failed to established a due diligence and in providing adequate checks and safeguard to prevent unauthorized access into his account. Bank had also not adhered to the KYC norms given by the RBI. The adjudicating officers directed the ICICI bank to pay damages to the petitioner under Section 43 of the IT Act.

4) The Bombay High Court has rejected a petition by the ICICI Bank Aug 29, 2012 - (L) No. 1236 of 2011 seeking stay on adjudicating an officer’s order to pay compensation to two persons who lost Rs5.41 lakh in online phishing attack.

Ramdas Pawar and Sourabh Jain, both residents of Pune, had moved the special court of state’s adjudicating officer, in 2011 for compensation. In September-October 2010, Rs3.39 lakh were illegally transferred from the accounts of Pawar. Similarly, Jain lost Rs2.02 lakh in October 2010. Pawar had account with the Bank’s Bund Garden Road branch while Jain had account in Shivajinagar branch. Both of them had lodged police complaints but the accused remained untraceable. Pawar and Jain’s lawyer Gaurav Jachak argued before the adjudicating officer that as per the Information Technology Act, it is mandatory for the bank to pay compensation.

The bank submitted to the court that “both the complainants had responded to phishing emails (asking about personal data) sent by fraudsters, and became victims of the online attack”. The case should have been against the beneficiaries of the transaction and not the bank, the bank argued. In February, the adjudicating officer Rajesh Agarwal passed the order in the complainants’ favour and ordered the bank to pay Rs1.5 lakh to Jain and Rs3 lakh to Pawar. The officer also ordered Idea Cellular to pay Rs25,000 to Jain for not following security practices before issuing duplicate SIM to another person.
The bank moved the Bombay High Court. However, the High Court upheld adjudicating officer’s judgment and rejected the bank’s petition and then review petition.

**3.4.3(D) PROBLEM OF MOUNTING CASES OF OFFENCES RELATED TO NETWORK SCANNING/PROBING**

**Network Scanning/Probing:** Network scanning is a procedure for identifying active hosts on a network, either for the purpose of attacking them or for network security assessment.

**YEAR WISE INCIDENTS OF NETWORK SCANNING/PROBING DURING 2004-2012**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Cyber Security Incidents</td>
<td>23</td>
<td>254</td>
<td>552</td>
<td>1237</td>
<td>2565</td>
<td>8266</td>
<td>10315</td>
<td>13301</td>
<td>22060</td>
</tr>
<tr>
<td>Network Scanning/Probing</td>
<td>11</td>
<td>40</td>
<td>177</td>
<td>223</td>
<td>265</td>
<td>303</td>
<td>277</td>
<td>1748</td>
<td>2866</td>
</tr>
</tbody>
</table>

**A) Observations on the mounting cyber crime cases related to Network Scanning/Probing**

As per Table No.8, the reported incidents of cyber crime cases related to Network Scanning/Probing were 13% as compared to total cyber security incidents reported during 2012. There was total rise of incidents of Network Scanning/Probing from 2004 to 2012 to the tune of 2855 and it gives the impression of inefficiency of law. There is a tremendous rise of cyber crime incidents of other offences including of offences of hacking and carders etc from 11 incidents in 2004 to 2866 incidents in 2012 as handled by CERTIn.

---

399 Source: - Annual Report of Asia Pacific Computer Emergency Response Team (2004-12)
B) LEGAL REMEDY AVAILABLE FOR OFFENCES RELATED WITH NETWORK SCANNING/ PROBING

Information Technology Act 2000 provisions against Network Scanning

Port scanning is used by mostly network and system administrators. Port scan has many legitimate uses including network inventory and the verification of the security of a network. Port scanning can, however, also be used to compromise security. exploits rely upon port scans to find open ports and send specific data patterns in an attempt to trigger a condition known as a buffer overflow.

Country specific provisions in IT laws for open and decentralized architecture of the Internet, lawmakers have struggled since its creation to define legal boundaries that permit effective prosecution of cyber criminal Network scanning: Although network scanning in legal but since its first step used by hackers boundary is unclear and there are implications for misuse.

At present the punishment for Network Scanning/probing is awarded under Information Technology (Amendment) Act,2000 vide Section 43(a) read with section 66 is applicable and Section 379 & 406 of Indian Penal Code, 1860.It is a cognizable and bailable offence. The offence is, compoundable with permission of the court before which the prosecution of such offence is pending and can be trial by any magistrate. Section 66 of the IT Act reads out:

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injurious by any means, commits hacking.

(2) Whoever commits the offence shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Data published by CERT-IN (Computer Emergency Response Team India) in this regards reflects that there is a tremendous rise of crime incidents within a span of nine years since 2004 to 2012 under this category. Therefore it gives the impression that there is no adequate and sufficient legal control of cyber crimes like Network Scanning/Probing against e-banking in India. However the IT Act appears sufficient in

400 http://sandyclassic.wordpress.com/2013/02/13/information-technology-laws-provisions-against-port-scanning
all respect but it is not competent enough to tackle the problems of such crimes because there are loopholes in the IT Act 2000 and other legislations and the criminals escape easily by taking the advantage of these loopholes. On the basis of the above our interpretation is that the existing cyber laws are inadequate and insufficient to control the cyber crimes against e-banking in India as there is a massive growth in cyber crime incidents.

C) INCIDENTS OF NETWORK SCANNING/PROBING ATTACKS AS FOLLOWS:-

1) 112 Government Websites Hacked In Last 3 Months; 1798 Internet Fraud Cases401:- Sachin Pilot, the Minister of State for Communication and Information Technology, INFORMED the Parliament of India, that a total of 112 Government websites were hacked during the period of December 2011 to February 2012. The hacked websites include websites of Government of Andhra Pradesh, Madhya Pradesh, Rajasthan, Tamil Nadu, Maharashtra, Gujarat, Kerala, Orissa, Uttar Pradesh, Sikkim, and Manipur along with the websites of Ministry of Finance, Health, Planning Commission and Human Resource Development. In addition to this announcement, Sachin Pilot also confirmed that Bharat Sanchar Nigam Limited (BSNL) was hacked by the Pakistani hacker group called ‘H4tr!ck’ on December 4, 2011 although he didn’t reveal the extent of damage caused.

2) Hackers hold bank to ransom over stolen data402

In an unusual move, a group of hackers has attempted to blackmail a Belgian bank for €150,000 over client data lifted from a compromised server A group of hackers has attempted to extort €150,000 from Belgian Bank Belfius by blackmailing the bank over hacked data. The hackers said in an online ransom note that if they were not paid within a prescribed time limit, they would release the data of customers of Elantis, taken from a compromised server. Elantis is a mortgage and consumer credit company owned by Belfius Bank. The hackers claimed to have accessed database tables containing unencrypted and unprotected data from loan applications such as applicants’ full

401 http://pib.nic.in/newsite/erelease.aspx?relid=80936
402 HTTP://pastebin.com/Squ.DtfUp
names, jobs, ID card numbers, contact information and details about their income. Belfius Bank told that it had informed the Federal Computer Crime Unit in Brussels and local police in Liege of the extortion attempt. Up to 3,700 customers and brokers may have been affected, and they have been informed of the probable breach, said the bank.

D) LEGAL CASES RELATED TO OFFENCES OF NETWORK SCANNING ATTACKS

1) Sony.Sambandh.Com Case

India saw its first cybercrime conviction recently. It all began after a complaint was filed by Sony India Private Ltd, which runs a website called www.sony-sambandh.com, targeting Non Resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online. The company undertakes to deliver the products to the concerned recipients. In May 2002, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless head phone. She gave her credit card number for payment and requested that the products be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency and the transaction processed.

After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim. At the time of delivery, the company took digital photographs showing the delivery being accepted by Arif Azim. The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase. The company lodged a complaint for online cheating at the Central Bureau of Investigation which registered a case under Section 418, 419 and 420 of the Indian Penal Code.

The matter was investigated into and Arif Azim was arrested. Investigations revealed that Arif Azim, while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company’s site. The CBI

---

403 http://www.alertindian.com/node/18
recovered the color television and the cordless head phone. In this matter, the CBI had evidence to prove their case and so the accused admitted his guilt. The court convicted Arif Azim under Section 418, 419 and 420 of the Indian Penal Code this being the first time that a cybercrime has been convicted.

The court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. The court therefore released the accused on probation for one year. The judgment is of immense significance for the entire nation. Besides being the first conviction in a cybercrime matter, it has shown that the Indian Penal Code can be effectively applied to certain categories of cyber crimes which are not covered under the Information Technology Act 2000. Secondly, a judgment of this sort sends out a clear message to all that the law cannot be taken for a ride.\(^{404}\)

2) Sandeep Varghese v/s State of Kerala

A complaint filed by the representative of a Company Jaya Polychem, which was engaged in the business of trading and distribution of petrochemicals in India and overseas. Under Sections 65, 66, 66A, C and D of the Information Technology Act along with Sections 419 and 420 of the Indian Penal Code a crime was registered against nine persons. The company owned a web-site in the name and and style \`www.jaypolychem.com but, another web site \`www.jayplychem.org was set up in the internet by first accused Samdeep Varghese @ Sam, in plan with other accused, including Preeti and Charanjeet Singh, sister and brother-in- law of accused. Sandeep Varghese was dismissed from the company Jaya Polychem. With the help of his sister & brother in law Sam Defamatory and malicious matters about the company and its directors were made available in the website www.jayplychem.org created by the accused . The accused sister and brother-in-law were based in Cochin and they had been acting in involvement who have jointly cheated the company and performed the acts of forgery, impersonation etc. The accused Sandeep Verghese and others sent e-mails from fake e-mail accounts of many of the customers, suppliers, Bank etc. to slander the name and image of the Company Jaya Polychem and its Directors. The

\(^{404}\) Talwant Singh Addl. District & Sessions Judge, Delhi
defamation movement run by all the accused persons has made massive dent to the name and status of the Company. Due to the movements against the company by the accused, The Company Jaya Polychem put up with the losses of crore of Rupees from its clients and customers and the company was pushed in a such a condition that the company was deprived of to do business.

3.4.3(E) PROBLEM OF MOUNTING CASES OF SPAM ATTACKS

Spamming:- The E-mail “spamming” refers to sending e-mails to users in bulk. It is similar to chain letter. Spamming is often done deliberately to use network resources. E-Mail Spamming may be combined with e-mail spoofing The spam is commonly called "brand spoofing" or "phishing" because the spam mail sent uses familiar or legitimate-sounding names of companies to trick consumers into disclosing confidential personal information. The email may use all or part of a legitimate company's name, and the hyperlink may closely resemble its website, complete with company logo and color schemes that make it look like close to the real thing. The emails received look like they may be coming from the company with whom you do business and even use a URL that looks like the real thing but it's not.

INCIDENTS OF SPAM ATTACKS DURING 2004-2012 IN INDIA  

<table>
<thead>
<tr>
<th>Year</th>
<th>Particulars</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>Total Cyber</td>
<td>23</td>
<td>254</td>
<td>552</td>
<td>1237</td>
<td>2565</td>
<td>8266</td>
<td>10315</td>
<td>13301</td>
<td>22060</td>
</tr>
<tr>
<td>2005</td>
<td>Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2006</td>
<td>Incidents</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td>Spam Attacks</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>305</td>
<td>285</td>
<td>181</td>
<td>2480</td>
<td>8150</td>
</tr>
<tr>
<td>2008</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A)Observations on the mounting cyber crime cases related to Spamming :- As per Table No.9, the reported incidents of cyber crime cases related to Spamming were 21% as compared to total cyber security incidents reported during 2012. There was total

---

405 Source: - Annual Report of Asia Pacific Computer Emergency Response Team (2004-12)
rise of incidents of Spamming from 2004 to 2012 to the tune of 5365 and it gives the impression of inefficiency of law. There is a tremendous rise of cyber crime incidents of spamming from 305 incidents in 2008 to 8150 incidents in 2012 as handled by CERT-In. The reported incidents of spamming were 37% as compared to total cyber security incidents reported during 2012.

B) LEGAL REMEDY AVAILABLE FOR OFFENCES RELATED WITH SPAMMING

Spamming Laws in India

As of today, the Indian government has yet to come out with a legislation that directly addresses the issue of spam. The Information Technology Act, 2000 (IT Act 2000) does not contain any provision regulating the act of spamming though it does regulate obscenity, which covers publishing, transmitting or causing to be published in electronic form any material which is lascivious, or appeals to the prurient interest. The Spam cases indirectly booked under Section 43 of Information Technology Act 2000. According to sources, the ministry pondered whether the punishment to spammers would be done after verifying the nature of the spam attack, that is, whether the act of spamming was done inadvertently or on purpose. The Indian Ministry of Information Technology had a discussion to incorporate a provision to have legislation against spammers. “This is a good development from the government. The ministry should create a panel and involve more technical people and experts from the IT industry when it plans to have legislation for cyber security and IT laws,” says Karnika Seth, attorney-at-law & partner, Seth Associates.

However, as of today in India, legal remedy is available under CAUSE (Coalition Against Unsolicited Commercial Email) India is available. It is a non-profit advocacy group that works to reduce the amount of unsolicited commercial email, or spam via legislation. CAUCE India was formed in the late 1990s.

Data published by CERT-IN (Computer Emergency Response Team India) in this regards reflects that there is a tremendous rise of crime incidents within a span of nine

406 http://www.lawyersclubindia.com/articles
years since 2004 to 2012 under this category. Therefore it gives the impression that there is no adequate and sufficient legal control of cyber crimes like Spamming against e-banking in India. However the IT Act appears sufficient in all respect but it is not competent enough to tackle the problems of such crimes because there are loopholes in the IT Act 2000 and other legislations and the criminals escape easily by taking the advantage of these loopholes. On the basis of the above our interpretation is that the existing cyber laws are inadequate and insufficient to control the cyber crimes against e-banking in India as there is a massive growth in cyber crime incidents.

C) INCIDENTS OF SPAM ATTACKS408:-
Among the early victims of spam in India are as under

1) Escorts MD Nikhil Nanda409, son-in-law of Amitabh Bachchan, was cheated into submitting his email ID, password and date of birth to a fake Microsoft account on July 21. The scamsters hacked two email accounts and his social network profile, and sought money from his contacts by impersonating him. The police are probing the complaint.

2) Income Tax return hoax410:- Also, each time the July 31 deadline for filing income-tax returns nears, the hoax about refunds is sent from web sites that are remarkably similar to the official portal. Fake links to Indian and foreign banks are provided and users are told to provide account numbers and passwords.

3) E-mail message from Reserve Bank of India411 :-Another scam involves the impersonation of outgoing Reserve Bank of India governor Dr D Subbarao. An e-mail purportedly sent by RBI offers to transfer $12 million (approximately Rs72 crore) to the receiver’s personal account. A Madhya Pradesh resident paid thousands of rupees after hearing that "Subbarao had met United Nations secretary general Ban Ki-moon to release funds".

408 The Times of India | Security | Bella Jaisinghani, TNN | Aug 7, 2013,
409 ibid
410 ibid
411 ibid
4) **Jiten Shah from Borivali**\(^{412}\) received an email from the 'Office of the permanent secretary for non residential taxation on international lottery award of the British Ministry of Finance, United Kingdom (sic). The letter offered him 500,000 pounds after he "cooperated" by paying 80 pounds as service charge. He trashed it right away.

5) **Atul Mishra from Satna, Madhya Pradesh**\(^{413}\): Among the early victims of spam was Atul Mishra from Satna, Madhya Pradesh, who transferred a substantial amount to a fraudster's account two years ago. Mishra told TOI over the telephone, "I received an email purportedly from RBI saying that I had won $1 million. It claimed I was the beneficiary of outstanding debts that the British government owed to India." Atul was told to pay "crediting fees" within two days to the account of Amit Kumar in New Delhi. He did, but when the windfall did not arrive, he realized he had been duped. Beset by multiple problems at that time, Mishra did not complain to the police or RBI. He merely uploaded his story on a consumer forum web site. "During those days, neither banks nor cell phone companies would send warning messages about phishing or internet fraud. The mail looked so real I succumbed to the hoax."

**Foreign Incidents of spam**

**Three banks process 95% of spam transactions**

When spam comes to banking, the bottlenecks are far more severe, and switching is far more difficult. One bank alone was used to settle more than 60 percent of all transactions, and the top three banks Azerigazbank in Azerbaijan, St Kitts & Nevis Anguilla National Bank in St Kitts & Nevis, and Norwegian-owned DnB Nord in Latvia— together accounted for more than 95 percent of all money paid to spam vendors. The implication is that many banks simply won't deal with spam outfits. Even when switching does occur, it's disruptive, with payment processors typically introducing delays of days or weeks for due diligence to be performed.

\(^{412}\) The Times of India | Security | Bella Jaisinghani, TNN | Aug 7, 2013

\(^{413}\) Ibid
The Latvian bank's Norwegian owners say that the spam customers were inherited when they bought the bank, and claim that they have terminated their relationship with the spam affiliate programs.414

**D) LEGAL CASE RELATED TO OFFENCES OF SPAM ATTACKS**

In India, the Information Technology Act, 2000 does not contain any provision regulating the act of spam. As of today, the Indian government has yet to come out with a legislation that directly addresses the issue of spam, hence there were no legal cases reported under SPAM.

**Following are the Foreign Law Suits as under:**

1) The first spam-related lawsuit was a small claims case filed by Robert Arkow against CompuServe in early 1995. Arkow had received unsolicited e-mail advertisements from Compu Serve. He argued that the federal law prohibiting unsolicited facsimile advertisements defined “facsimile machine” broadly enough to include computers that send and receive electronic mail. The parties settled out of court and the terms were never disclosed. Thus, the applicability of the law governing the use of facsimile machines to e-mail has never been formally adjudicated.

2) LinkedIn sued for 'hacking' users' email accounts415

Four LinkedIn users have filed a lawsuit accusing the business-oriented social network of accessing their email accounts without permission, harvesting the addresses of their contacts and spamming those people with repeated invitations to join the service. In their most explosive claim, the plaintiffs say that LinkedIn is "breaking into" external email accounts, like Gmail or Yahoo Mail, by pretending to be the account owner, although the legal complaint offers no details about that assertion. Larry Russ, a lawyer for the plaintiffs, declined to comment beyond the suit.

The lawsuit, which is seeking damages on behalf of all LinkedIn users, revives a long-standing issue about the service: Does LinkedIn adequately inform its users about how it uses sensitive information, including email addresses of everyone they know, and get their consent to do so

---

414 Peter Bright in his article “A way to take out spammers? banks process 95% of spam transactions” on June 1, 2011. Source http://arstechnica.com/tech-policy/2011/05/

415 The Times of India | Internet | Vindu Goel, New York Times | Sep 23, 2013
3.4.3(F) PROBLEM OF MOUNTING CASES RELATED TO OTHER OFFENCES INCLUDING OFFENCES OF HACKING/ CARDERS ETC.

Hacking: - Attackers use sophisticated programming techniques to break into websites which reside on a financial institution's network. Using this access, they can access the bank's systems.

Carders: - "Carders" are the people who buy, sell, and trade online the credit card data stolen from phishing sites or from large data breaches at retail stores.

YEARWISE INCIDENTS OF OTHER OFFENCES IN INDIA DURING 2004-2012

<table>
<thead>
<tr>
<th>Year</th>
<th>Incidents</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Cyber Security Incidents</td>
<td>23</td>
<td>254</td>
<td>552</td>
<td>1237</td>
<td>2565</td>
<td>8266</td>
<td>10315</td>
<td>13301</td>
<td>22060</td>
<td></td>
</tr>
<tr>
<td>Other Offences related with cyber crimes</td>
<td>4</td>
<td>18</td>
<td>17</td>
<td>264</td>
<td>148</td>
<td>160</td>
<td>188</td>
<td>1240</td>
<td>2417</td>
<td></td>
</tr>
</tbody>
</table>

A) Observations on the mounting cyber crime cases related to other offences including of offences of hacking and carders etc:- As per Table No.7, the reported incidents of other offences including of offences of hacking and carders etc were 11 % as compared to total cyber security incidents reported during 2012. There was total rise of incidents of other offences including of offences of hacking and carders etc from 2004 to 2012 to the tune of 2413 and it gives the impression of inefficiency of law. There is a tremendous rise of cyber crime incidents of other offences including of offences of hacking and carders etc from 4 incidents in 2004 to 2417 incidents in 2012 as handled by CERTIN.

416 Source: - Annual Report of Asia Pacific Computer Emergency Response Team (2004-12)
B) LEGAL REMEDY AVAILABLE FOR OFFENCES RELATED WITH HACKING

Law & Punishment: Under Information Technology (Amendment) Act, 2008, Section 43(a) read with section 66 is applicable and Section 379 & 406 of Indian Penal Code, 1860 also are applicable. If crime is proved under IT Act, accused shall be punished for imprisonment, which may extend to three years or with fine, which may extend to five lakh rupees or both. Hacking offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

Section 43(a) read with section 66 in The Information Technology (Amendment) Act, 2008:-

Section 43(a) in the ITAA 2008:- Under this section the body corporate shall be liable to pay compensation if it is negligent in implementing “reasonable security precautions” with respect to “sensitive personal data”. The liability would arise if the negligence leads to a wrongful loss or wrongful gain to a person (43A).

Section 66 ITAA Act 2008: Section 66 Information Technology Act is applicable when a person dishonestly or fraudulently, does any act referred to in section 43 which contains mainly ten acts which mainly comprises of downloading, copying from computer without permission, introducing virus or contaminant, hacking etc.

Section 379 in The Indian Penal Code, 1860, "Punishment for theft":- Whoever commits theft shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

Section 406 in The Indian Penal Code, 1860: Punishment for criminal breach of trust:- Whoever commits criminal breach of trust shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

Data published by CERT-IN (Computer Emergency Response Team India) in this regards reflects that there is a tremendous rise of crime incidents within a span of nine years since 2004 to 2012 under this category. Therefore it gives the impression that there is no adequate and sufficient legal control of cyber crimes like hacking against e-
banking in India. However the IT Act appears sufficient in all respect but it is not competent enough to tackle the problems of such crimes because there are loopholes in the IT Act 2000 and other legislations and the criminals escape easily by taking the advantage of these loopholes. On the basis of the above our interpretation is that the existing cyber laws are inadequate and insufficient to control the cyber crimes against e-banking in India as there is a massive growth in cyber crime incidents

C) INCIDENTS OF OTHER OFFENCES INCLUDING HACKING ATTACKS AS FOLLOW:

1) Online Credit card fraud on e-bay\(^{417}\): Rourkela police busted a racket involving an online fraud worth Rs 12.5 lakh. The modus operandi of the accused was to hack into the eBay India website and make purchases in the names of credit cardholders. Two persons, including alleged mastermind Debasis Pandit, a BCA student, were arrested and forwarded to the court of the sub divisional judicial magistrate, Rourkela. The other arrested person is Rabi Narayan Sahu. The duo was later remanded in judicial custody but four other persons allegedly involved in the racket were untraceable. A case has been registered against the accused under Sections 420 and 34 of the Indian Penal Code and Section 66 of the IT Act and further investigation is on. Sahu, his associate and a constable, was nabbed at his house in Uditnagar. Pandit allegedly hacked into the eBay India site and gathered the details of around 700 credit cardholders. He then made purchases by using their passwords. The fraud came to the notice of eBay officials when it was detected that several purchases were made from Rourkela while the customers were based in cities such as Bangalore, Baroda and Jaipur and even London. The company brought the matter to the notice of Rourkela police after some customers lodged complaints.

2) Hackers target bank web sites, steal crore\(^{418}\): A gang of crooks fraudulently obtained customer data by hacking into bank websites and used it to empty their accounts, police said. While the kingpin of the gang has been arrested, his aides, including a hacker, an accountancy specialist and a bank operations expert, have been

\(^{417}\) http://www.cyberlawsindia.net/cases2.html
identified and teams have gone to several states to nab them. The accused targeted foreign customers to avoid complaints in India. The total amount siphoned by these crooks is suspected to be in the tune of several crore. The possible involvement of bank personnel is also being ascertained and cops are investigating how banks issued card swiping machines without proper verification of the merchant.

"The kingpin, Arun Kumar (30), belongs to Kannouj in Uttar Pradesh and was living in Mayur Vihar Seven card swiping machines and 26 cheque books of different banks, fake seals, 10 PAN cards and four debit cards have been found. The others involved in the fraud have been identified as Yasin, Jitender, Vikas and Sanjeev," They planned to prepare clones of credit and debit cards to earn quick money. The accountancy specialist then formed several fake e-companies and used them to get the card swiping machines allotted. The gang also opened bank accounts using forged documents which were linked to the machines. Yasin first entered the bank's website and transferred customer data to the data readers. These data readers were attached to the cloning machines which copied the data onto blank cards."The gang swiped the cards on the swiping machines allotted by the banks which transferred money to their accounts. This money was immediately withdrawn at ATMs and through cheque books," On August 5, the chief manager of a bank in Nehru Place filed a complaint regarding an incident of cheating by the owner of a company called Blue Waves Technology. Similar incidents had been reported in parts of Delhi and NCR. Investigations revealed that Arun Kumar owned Blue Waves and that he had recently moved his office from Kalkaji to Govindpuri. On August 7, a trap was laid with help of bank officials and Arun was apprehended.

3) SMS Scam Accused arrested by police

Two brothers namely Nadar along with their friend Ramesh Gala, took help of SMS technology and launched the first of it's kind SMS fraud in India. They launched a campaign in print media & also put up a website (www.getpaid4sms.com) wherein subscribers were asked to pay deposit of INR 500 and they receive 10 SMS every day against it. The customers were promised handsome commissions if they managed to rope in more subscribers by forwarding the messages.

419 http://www.cyberlawsindia.net/cases1.html
Nadar Brothers told their customers that they were working for a US based company called Aropis Advertising Company which wanted to conduct a market survey about local response to their advertisement and were using SMS as it was the latest means of communication.
Initially small amounts were paid but when large amounts of cheques began to get dishonored the customers’ starded to worry. On November 30, one of the duped agents approached the DN Road police station and lodged a complaint after a bank failed to honour a pay order amounting Rs.2.17 million issued by the Nadar brothers.
A case was registered with the DN Nagar Police station & later transferred to Economic Offences Wing (EOW).

4) Two Nigerians held for financial fraud
Two Nigerians wanted in connection with a banking fraud case reported in Tamil Nadu few months back have been arrested by the South District Police.
It was alleged that the arrested men were both part of an international online hacking network, the members of which send a Malware affected attachment after accessing email addresses of bank customers. According to the police, when a customer downloaded the virus affected attachments, it created a parallel folder of that customer with the hacker.
“Thereafter, whenever the customer used net banking, his information was stored in the hacker’s computer also and was used by the hackers to access the customer’s bank account. The hackers would also get the mobile number of the customer blocked so that no SMS alert could be received by him or her. So far they have targeted 500 account holders and the laptops seized from them contained data of more than 1.5 crore accounts from almost all the major banks across the country,” said a senior police officer.
One such victim, Subramanium Mohan, a resident of Coimbatore, approached the local police informing them that an amount of Rs.70 lakh was debited from his NRI account

and transferred to three different accounts, one of them based in China. On the basis of Mr. Mohan’s complaint a case was registered at Coimbatore City Cyber Cell. During the police investigation it was found that two banks accounts in India, where a part of the money debited from Mr. Mohan's account was deposited, were held by M/s R.P Enterprises and Sujata Traders. On verification, beneficiaries of the cheated amount were found to be Rajesh Pandey of M/s R.P Enterprises, Badarpur, Delhi and Vivek of M/s Sujata Traders at Faridabad, Haryana. It was also found that the know your customer (KYC) document submitted to the bank by account holders and addresses given by them were verified and were found to be fake. The police then perused the account statements which revealed that amount deposited in the said accounts was being withdrawn through ATMs. With the help of the phone number used to call the bank manager Faridabad Police arrested Roland Chukwudi Alumona and Stanley Ransome Ogwu and arrested them from Raju Park New Delhi.

D) LEGAL CASES RELATED TO OFFENCES OF HACKING ATTACKS

1) Sanjay Kumar vs. State of Haryana on 10th Jan, 2013 CRR No.66 of 2013 (O&M)421

(Punjab-Haryana High Court (Section 65 and Section 66 of the IT Act, 2000)

Present criminal revision has been preferred by the petitioner against judgment dated 21.08.2012 passed by the learned Sessions Judge, Faridabad, whereby an appeal preferred by the petitioner has been dismissed and judgment of conviction dated 01.09.2011 and order of sentence dated 03.09.2011 passed by learned Judicial Magistrate First CRR No.66 of 2013 (O&M) 2 Class, Faridabad, has been upheld, vide which the petitioner has been convicted for offences punishable under Sections 420, 467, 468, 471 of the Indian Penal Code and Sections 65 and 66 of the Information & Technology Act, 2000 and sentenced to undergo rigorous imprisonment as follows:-

"Under Section Period Fine 420 IPC Two years Rs.1,000/- 467 IPC Three years Rs.2,000/- 468 IPC Two years Rs.1,000/- 471 IPC Two years Rs.1,000/- 65 I.T. Act Two years Rs.1,000/- 66 I.T. Act Two years Rs.1000/- In default of payment of fine, the

421 http://www.indiankanoon.org/doc/70806873
petitioner shall further undergo simple imprisonment for a period of two months. All the sentences were ordered to run concurrently”.

**Brief facts of the case:-** The Senior Branch Manager, Vijaya Bank, NIT, Faridabad moved a complaint dated 11.02.2003 before the Police stating that the petitioner was deputed by M/s Virmati Software and Telecommunication Ltd. to maintain the Software System supplied by them to the bank. He was also looking Software System of certain other banks. In connection with rendering such services, the petitioner was having access to their accounting system which was computerized and was also in a position to enter into ledgers and various other accounts. While reconciling the accounts, certain discrepancies were pointed out by the officials of the bank and in that process, it was revealed that the accused-petitioner, who was having SB Account No. 21499 in his CRR No.66 of 2013 (O&M) 3 personal name in their bank, manipulated the entries by forging and fabricating certain entries from one account to another, from the computer system by handling the software and got the entries pertaining to the amount of the the bank and withdrew the amounts from the bank on various dates by issuing cheques in his own favour and withdrew the amount from the cash counter of the bank as well as through transfer/clearing transactions. As per enquiry, it has been revealed that the accused by carrying out forgery, fabricating the entries in the computer system of the bank, illegally and wrongfully, withdrew Rs.17, 67,409/- from the bank and thus, caused wrongful gain to himself and wrongful loss to the bank. The said Bank came to know regarding the fraud committed by the accused on 07.02.2003. thereafter, the accused was called to the bank and he was confronted with the details of the fraud but he gave evasive replies as only admitted having embezzled a sum of Rs. 17 lacs without giving further information or revealing the exact amount of fraud or the modus operandi of the same and also assured to pay back the amount to the bank. On receipt of the complaint, a case bearing FIR No. 165 dated 11.02.2003, under Sections 406, 420, 467, 468, 469, 471 of the Indian Penal Code and Sections 65, 66 and 72 of the Information and Technology Act, 2000 was registered against the petitioner. Thereafter, charge was framed against the accused petitioner to which he pleaded not guilty and claimed trial. The learned trial Court, after appreciation of the evidence, convicted and sentenced the petitioner as aforesaid vide judgment and order dated 01.09.2011 and
03.09.2011 respectively. Thereafter, the petitioner preferred an appeal, which was dismissed by the learned Sessions Judge, Faridabad vide judgment dated 21.08.2012. Hence, this criminal revision


The accused is the CEO of Baaze.com, which Company facilitates the sale of any property, for which it receives commission and also generates revenue from advertisement carried on its web page. In this case, Counsel for the State has argued that the accused was remiss, at the pain of culpability, in not stopping payment through Banking channels after learning of the illegal nature of the transaction. It has been strenuously contended that if bail is not granted it will adversely impact e-commerce, for which India may be the eventual loser. These are not considerations which India may be the eventual loser. These are not considerations which would prevail or tamper the Courts decision whether to grant or reject bail. Mr. Jaitely, counsel for the petitioner has underscored that in Section 67 of the Information Technology Act, 2000, an offence is committed by a person who publishes or transmits any material which is lascivious or appeals to the prurient or transmits any material which is lascivious or appeals to the prurient interest. Sections 292 and 294 of the Indian Penal Code have also been mentioned which contemplate the selling, letting on hire, distribution public exhibition of the absence matter. He has emphasized that the provision does not bring within its sweep the causing of the transmission in contradistinction to the publication of obscene material. Prima facie it has not been established from the evidence that has been gathered till date that any publication took place by the accused, directly or indirectly. The actual obscene recording/clip cannot be viewed on the portal of Bazze.com. It was held that the accused has actively participated in the investigations, and nothing was even argued before it in contrary by Counsel for the State. The nature of the alleged offence is such that the evidence has already crystallized and may even be tamper proof. Even though the accused is no longer an Indian National, he is of Indian origin with family roots in our country. It cannot possibly be argued that a foreign national is disentitled to the grant of bail. The accused is enlarged on bail subject to furnishing two sureties in the sum of Rs. 1,00,000/- each to the satisfaction of the concerned Court/ Metropolitan

422 150(2008)DLT769, 2008(105)DRJ721
Magistrate/Duty Magistrate. The Accused shall also not leave the territories of India without
the leave of the Court and far for this purpose shall surrender his passport to the
Magistrate. It is implicit in the grant of bail that he shall participate and assist in the
investigation. The Bail Application stands disposed off.

3) Nirav Navinbhai Shah & 4 Ors. v State of Gujarat and Anr. (In The High Court of
Gujarat)\(^\text{423}\)

The applicants, original accused in crime I.C.R. No. 54 of 2004 dated 26.02.2004
registered with sector 7 police station Gandhinagar for offences punishable under sections
381, 408, 415, 418, 420 read with sections 34 and 120B of the Indian Penal Code and
section 66 and 72 of the Information Technology Act, 2000 (herein after referred to as ‘the
IT Act for short) have preferred this application under section 482 of the Code of Criminal
Procedure 1973 (herein after referred to as ‘the code’ for short) for quashing of FIR I.C.R.
No. 54 of 2004 dated 26.02.2004 registered with Sector No. 7 Police Station Gandhinagar
and the resultant Criminal Case No. 54 of 2004 dated 26.02.2004 registered with sector
No. 7 Police station Gandhinagar and the resultant Criminal case No.3528 of 2004 pending
before the judicial Magistrate First Class Gandhinagar, mainly on the grounds that the facts
and allegation leading to lodging FIR show that the real dispute was a civil dispute and as
the same has been amicably settled between the parties, no useful purpose would be
served in continuing the criminal proceedings, rather continuation of same would be
counterproductive to the interest of justice.

The compliant also does not contain any essential ingredient for maintaining criminal
proceeding for the alleged offences. As its stated in the arguments of the learned counsels
that the parties have filed civil suits also in respect of the same dispute. The entire dispute
between the parties is resolved by amicable settlement. The alleged hacking is perpetrated
on the Complainants computer system only which said to have data pertaining to its client.
The Counsels have submitted that on sale of the web sites these data are already
available. The dispute appears to be private in nature. The offence alleged is not strictly
affecting or infringing any other individual or citizen. Thus looking to the nature of the
disputes, it can well be said that continuation of the same is not in interest of justice. It was

\(^\text{423}\) http://indiankanoon.org/doc/1119978/
held that the FIR 54 of 2004 registered at sector 7 Police Station Gandhinagar and resultant Criminal Case No. 3528 of 2004 pending before the JMFC Gandhinagar deserve to be quashed in the interest of just and hereby they are quashed. Rule is made absolute.

4) State of Maharashtra v/s Anand Ashok Khare\(^{424}\)

**Brief of the case:** This case related to the activities of the 23-year-old Telecom engineer Anand Ashok Khare from Mumbai who posed as the famous hacker Dr Neuker and made several attempts to hack the Mumbai police Cyber Cell website.

On 5th July 2001 the website of the Cyber Crimes Investigation Cell Mumbai was hacked by Anand Ashok Khare. Mumbai Police identified the hackers who hacked and changed the homepage of the Mumbai Police website. Police investigation reveals that it was a cyber cafe i.e. “Osprey Enterprises” at Dadar in Mumbai. Shivaji Park Police Station search the copy of the homepage in a computer which was replaced by the culprit. Mumbai police seized that computer under the provisions of IT Act 2000. After investigation the police arrested Anand Ashok Khare and Mahesh Mhatre for committing hacking. The duo accepted their crime. Presently they are working with Mumbai Police to fight back with cyber crime.

5) Washington Post v. Total News. 97 CIF. 1190 (PKL)\(^{425}\).

**History of the case:** Where the "totalnews.com" website used framing technology to set a news story from other website within the overall Total News frame by blocking banner advertisements and other distinguishing features.

The U.S. District Court Southern District of New York passed an order of settlement stating that “the defendants agree permanently to cease the practice of framing plaintiff's websites”. Plaintiffs agree that Defendants may link from the Totalnewa.com website or any other website to any plaintiff's website provided that:

a) Defendants may link to plaintiff's website only via hyperlinks consisting of the names of the linked sites in plain text, which may be highlighted;

\(^{424}\) http://www.cyberlawconsulting.com/cyber-cases.html  
\(^{425}\) http://www.cyberlawconsulting.com/cyber-cases.html
b) Defendants may not use on any website, as hyperlinks or in any other way, any of plaintiff's proprietary logos or other distinctive graphics, video or audio material, nor may defendants otherwise link in any manner reasonably likely to:

(i) imply affiliation with, endorsement or sponsorship by any plaintiff;

(ii) cause confusion, mistake or deception;

(iii) dilute Plaintiff's marks; or

(iv) otherwise violate state or federal law;

d) Each plaintiff's agreement to permit linking by defendants remains revocable, on 15 business days notice, at each Plaintiff's sole discretion. Revocation by any plaintiff shall not affect any other terms and conditions set forth herein. If defendants refuse to cease linking upon notice, and any plaintiff brings an action to enforce its rights under this subparagraph, it shall be an affirmative defense that defendants conduct does not otherwise infringe or violate plaintiff's rights under any theory of any intellectual property, unfair competition or other law.

7) Pune Citibank MphasiS Call Center Fraud

US $3,50,000 from accounts of four US customers were dishonestly transferred to bogus accounts. All accounts were opened in Pune and the customers complained that the money from their accounts was transferred to Pune accounts and that’s how the criminals were traced. It is a case of sourcing engineering. Some employees gained the confidence of the customer and obtained their PIN numbers to commit fraud. They got these under the guise of helping the customers out of difficult situations. They defrauded the United States based Citibank customers of more than Rs. 1.5 crore, including damage to data. One of the victims then lodged complaint to the Citibank and then Citibank alerted the Mumbai and New York City Investigative Services Mumbai Citigroup immediately reached recipient banks in Pune and alerted the Pune Police’s Cyber Crime Cell to trap the cyber fraud. The accused were caught red-handed while they were about to check the fund transfer in a Rupees Co-operative Bank, Pune. The accused were charged u/s 65, 66, 71 and 72 of the IT Act, 2000 and u/s 420, 465, 467 and 671 of the IPC, 1860.

3.4.3(G) PROBLEM OF MONEY LAUNDERING IN INDIAN BANKING

Money Laundering: - It is the process of changing large amounts of money that have been gained through illegitimate means. Money evidently gained through crime is "dirty" money, and money that has been "laundered" to appear as if it came from a legitimate source is "clean" money by using the bank

YEARWISE MONEY LAUNDERING CASES OF SEARCH/SEIZURES BY ENFORCEMENT DEPARTMENT DURING 2004-2012

Table 3.22- Money Laundering Cases of Searches /Seizures during 2004-2012 (Amt in Crore)427

<table>
<thead>
<tr>
<th>Year</th>
<th>No. of Searches /Raids</th>
<th>No. of Seizures/ Recoveries</th>
<th>Indian Currency Seized</th>
<th>Foreign Currency Seized</th>
<th>Indian Currency Confiscated</th>
<th>Foreign Currency Confiscated</th>
<th>FINE Imposed</th>
<th>Fine Released</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Searches /Raids</td>
<td>78</td>
<td>146</td>
<td>51</td>
<td>108</td>
<td>95</td>
<td>110</td>
<td>123</td>
<td>72</td>
</tr>
<tr>
<td>No of Seizures/ Recoveries</td>
<td>56</td>
<td>106</td>
<td>44</td>
<td>74</td>
<td>76</td>
<td>79</td>
<td>74</td>
<td>59</td>
</tr>
<tr>
<td>Indian Currency Seized</td>
<td>2.60</td>
<td>9.73</td>
<td>4.87</td>
<td>11.16</td>
<td>16.42</td>
<td>17.15</td>
<td>11.74</td>
<td>18.30</td>
</tr>
<tr>
<td>Foreign Currency Seized</td>
<td>0.40</td>
<td>0.40</td>
<td>0.38</td>
<td>0.55</td>
<td>1.00</td>
<td>5.44</td>
<td>0.78</td>
<td>7.27</td>
</tr>
<tr>
<td>Indian Currency Confiscated</td>
<td>6.00</td>
<td>3.95</td>
<td>0.98</td>
<td>2.22</td>
<td>2.33</td>
<td>5.77</td>
<td>1.73</td>
<td>2.27</td>
</tr>
<tr>
<td>Foreign Currency Confiscated</td>
<td>6.90</td>
<td>1.55</td>
<td>0.41</td>
<td>0.08</td>
<td>0.28</td>
<td>2.36</td>
<td>0.49</td>
<td>27.80</td>
</tr>
<tr>
<td>FINE Imposed</td>
<td>2518.70</td>
<td>1454.60</td>
<td>6.00</td>
<td>527.71</td>
<td>220.80</td>
<td>3645.32</td>
<td>566.66</td>
<td>323.45</td>
</tr>
<tr>
<td>Fine Released</td>
<td>20.00</td>
<td>11.04</td>
<td>9.06</td>
<td>18.15</td>
<td>15.45</td>
<td>12.21</td>
<td>7.70</td>
<td>15.78</td>
</tr>
</tbody>
</table>

A) OBSERVATION ON CYBER CRIME INCIDENTS:- Enforcement Directorate conducted total 801 Searches/Raids and 584 Seizures/Recoveries in money laundering

427 Source: http://ncrb.gov.in/
cases from FY2004 to FY2012. During FY2004 to FY2012 Indian currency seized by Enforcement Directorate in money laundering cases to the tune of Rs.95.67 crore and foreign currency seized equivalent to Indian Rs. 17.12 crore. During the span of nine years i.e. from FY2004 to FY2012 in money laundering cases, Enforcement Directorate confiscated total Rs.26.62 crore in Indian currency while foreign currency confiscated equivalent to Indian Rs. 40.24 crore. During the period Enforcement Directorate imposed fine in money laundering cases to the tune of Rs. 9271.85 crore while fine released to the tune of Rs.109.97 crore by Enforcement Directorate. It reveals from the above table there is a control of law on the reported incidents. But the directorate department could not trace out the incidents of money laundering.

B) LEGAL REMEDY AVAILABLE FOR OFFENCES OF MONEY LAUNDERING

1) Information Technology Act 2000 provisions against Money Laundering

The offences under this category are temporarily keeping a web service for collecting money illegally without registering with the any regulating authority for avoiding tax. The incidents of money laundering are dealt with section43, 65, 66 and 72 of Information Technology Act

2) Prevention of Money Laundering Act, 2002(PMLA2002)\(^{428}\)

Prevention of Money Laundering Act is Indian law passed in 2002 to prevent money-laundering and to provide for confiscation of property derived from money-laundering.

i) Punishment for money-laundering

The act prescribes that any person found guilty of money-laundering shall be punishable with rigorous imprisonment from three years to seven years. He could also be liable to fine of up to ₹500000 (US$7,700)\(^{429}\) However, vide amendment of PMLA, 2002 in 2012; the upper ceiling on the quantum of fine has been done away with.

ii) Special courts

The trial for the offences mentioned in the act are conducted by a special court, also called "PMLA Court". The Central Government (in consultation with the Chief Justice of the High Court) designates a Sessions Court as Special Court. Any appeal against order passed by PMLA court can directly be filed in the High Court (for that jurisdiction).

\(^{428}\) From Wikipedia, the free encyclopedia

\(^{429}\) Section 4 in PMLA, 2004

301
3) Statutes prior to enactment of PMLA2002


4) PMLA (Amendment) Act 2012\(^{430}\)

The PMLA was enacted in 2002, but was amended thrice, first in 2005, then in 2009 and then 2012. The 2012 version of the amendment received president's assent on January 3, 2013, and the law became operational from February 15, when the finance ministry notified it.

The government's argument is that it had to amend the existing law once more as India became a member of the Financial Action Task Force (FATF) in October 2010. Headquartered in Paris, the FATF is an inter-governmental body that promotes policies to combat money laundering and terrorist financing. And it was the FATF that pointed out a few deficiencies in India's anti-money-laundering legislation.

However the IT Act appears sufficient in all respect but it is not competent enough to tackle the problems of such crimes because there are loopholes in the IT Act 2000 and other legislations and the criminals escape easily by taking the advantage of these loopholes. Therefore it gives the impression that there is no adequate and sufficient legal control of cyber crimes like Money Laundering in Indian banking. On the basis of the above we interpret that the existing cyber laws are inadequate and insufficient to control the cyber crimes against e-banking in India as there is a massive growth in cyber crime incidents.

\(^{430}\) From Wikipedia, the free encyclopedia
C) INCIDENTS of MONEY LAUNDERING CASES AS UNDER

1) 23 public & private sector banks and insurance companies involved in money laundering

As many as 23 public and private sector banks and insurance companies were Monday accused of "running a nation-wide money laundering racket, blatantly violating laws of the land" by online portal Cobra post.

Cobra post alleged that the financial sector entities offered to open bank accounts and lockers for customers without following Know Your Customer (KYC) norms, convert their black money into white and obtain fictitious PAN cards.


This is the second expose by Cobra post. Earlier on March 14, it had alleged money laundering by top private sector banks -- HDFC Bank, ICICI Bank and Axis Bank.

Talking to reporters, State Bank of India (SBI) Chairman Pratip Chaudhuri said the bank would investigate the allegations and take severe action against those found guilty. "So far, it does not indicate if KYC violations have been done. But if they have been done, the people would be severely punished," he said. "We are very clear that there is zero tolerance for any money laundering or working around the KYC."

2) HSBC to pay $1.9B to settle money-laundering case

Europe's largest bank by market value, HSBC, has avoided a legal battle that could further savage its reputation and undermine confidence in the global banking system by agreeing Tuesday to pay $1.9 billion to settle a U.S. money-laundering probe.

HSBC will pay the biggest penalty ever imposed on a bank after facing accusations it transferred funds through the U.S. from Mexican drug cartels and on behalf of nations such as Iran that are under international sanctions.

---

431 Kobra Post May 07, 2013 on Zee News
432 The Associated Press

303
3) Bank of Credit and Commerce International (BCCI) case of money laundering

At its peak, the Bank of Credit and Commerce International (BCCI) was the seventh largest private bank in the world. However, during the mid-1980s the bank was found to be involved in various fraudulent activities including massive amounts of money laundering. Billions in criminal profits, including drug money, went through its accounts. The bank was not too picky about its customers, either: clients included Saddam Hussein, former military dictator of Panama Manuel Noriega, and Palestinian terrorist leader Abu Nidal. It has also been alleged that the CIA used accounts at the BCCI to fund the Afghan Mujahedeen during their war with the Soviet Union in the 1980s.

4) Indian-origin men jailed for money laundering in UK

Two Indian origin men have been jailed for their alleged involvement in a multi-million pound money laundering scam following an operation by Britain’s National Crime Agency official said 34 years old Amin Surnani was arrested as he collected 50,000 lbs from co-conspirator Surinder Rahela at a barber’s shop in the Green South hall, on May 9, 2013.

Another 10,000 lbs was found in Surnani’s possession, while a search of his home address uncovered a further 1,00,000 lbs besides a diary detailing his other dealings. The ability to launder the proceeds of their crimes is a pre-requisite for those involved in sophisticated criminal activity. Surnani was a familiarized money launderer and acted as a collector for other criminal networks. The investigations of the Britain’s National Crime Agency showed that in the four months prior to his arrest around 4.5 million lbs had passed through his operation. It is likely that much of this money was linked to drug trafficking.

---

433 Wikipedia, the free encyclopedia
434 Prasun Sonwalkar, Hindustan TimesLondon
After a two weeks trial at the Old Bailey, Surnani was found guilty on two counts of money laundering. He was sentenced to six and a half years in prison and faces deportation to India at the end of his sentence. Rahela 61 was found guilty of one count on money laundering and jailed for 18 months.

**D) LEGAL CASE RELATED TO OFFENCE OF MONEY LAUNDERING**


While the Indian Bank has come up with the first writ petition challenging a provisional order of attachment passed by the Joint Director of Enforcement, the Company whose property was so attached has come up with the second writ petition challenging the provisional attachment well as a consequent complaint lodged with the Adjudicating Authority.

The petitioner in the first writ petition is the Indian Bank and the petitioner in the second writ petition is a company, which borrowed monies from the Indian Bank. The factual matrix, out of which the present writ petitions arises, is as follows:-

i) The petitioner in the second writ petition was sanctioned 3 term loans, dated 2.1.2006 by the Indian Bank. With the money so advanced by the Indian Bank, the petitioner in the second writ petition, purchased a property at St. Thomas Mount, Chennai-16,

(ii) On 31.1.2008, the Indian Bank lodged a complaint with the Superintendent of Police, Central Bureau of Investigation against the company, alleging that the company and the officers of the company had defrauded the Bank.

(iii) Similarly, the State Bank of India lodged a complaint alleging that the company organised personal loans for 161 persons, showing them as its employees. This complaint was lodged on 14.11.2008.
(iv) The Bank of India lodged another complaint on 29.9.2008, alleging that the company obtained loans under Star Personal Loan Scheme in the name of 149 persons allegedly employed by them.

(v) On the complaint lodged by the Indian Bank, a charge sheet was filed in No.21/2008 on the file of the Additional Chief Metropolitan Magistrate, Egmore, Chennai. Another charge sheet was laid in No.9/2009 on 11.12.2009 in respect of the complaint filed by the State Bank of India. The charge sheet alleged that the company and one Mr. S. Senthilkumar, who is its Managing Director, had committed offences punishable under Sections 120-B, 420, 467, 468 and 471 of the Indian Penal Code.

(vi) The charges framed against the company and its officers also included the offences indicated in the Schedule in terms of Section 2(1)(y) of the Prevention of Money Laundering Act, 2002.

(vii) Thereafter, the Joint Director of Enforcement passed an order bearing No.01/2012 on 22.2.2012 under Section 5(1) of the Prevention of Money Laundering Act, 2002, directing the provisional attachment of the aforesaid property at St. Thomas Mount, Chennai-16.

(viii) Immediately upon coming to know of the said order of provisional attachment, the Indian Bank came up with the above writ petition W.P.No.4696 of 2012, contending that the account of the company had already become a non-performing asset and that since the property was mortgaged to them, the Bank had already taken steps to bring the property to sale in terms of the provisions of the SARFAESI Act, 2002. The prayer in the writ petition was to quash the provisional order of attachment.

(ix) Pending disposal of the writ petition, the Indian Bank also sought an interim stay of all further proceedings pursuant to the provisional order of attachment, in M.P.No.1 of 2012.

(x) As per Section 5(1) of the Act, the provisional attachment order passed by the Directorate of Enforcement can be in force only for a period of 150 days. But within 30 days, the Directorate can seek a confirmation of the order from the Adjudicating Authority under Section 8. Therefore, the Director of Enforcement filed an application before the Adjudicating Authority and the same was taken on file in O.C.No.129/2012 and notice was issued to the company and its Managing Director.
3.4.3(H) PROBLEM OF MOUNTING OF CYBER FRAUD CASES IN BANKING SECTOR IN INDIA

Fiscal Fraud: Internet banking fraud is a fraud or theft committed using online technology to illegally remove money out of your account. Internet banking fraud is a form of identity theft and is usually made possible through techniques such as phishing.

FRAUDS IN THE BANKING SECTOR

The reporting of fraud cases by banks was prescribed by RBI way back in July 1970. In 2005-06, the prescription of reporting of fraud cases was extended to urban cooperative banks and deposit taking NBFCs registered with RBI. In March 2012, NBFC-ND-SIs (systemically important, non-deposit taking NBFCs) having asset base of Rs. 100 crore and above were also brought under the reporting requirements. While online reporting and monitoring of fraud cases by the banks has been in place since May 2004, the reporting by UCBs and NBFCs is still in manual format.

A1) COMMERCIAL BANKS-FRAUD CASES & AMOUNT INVOLVED-31/03/2013

<table>
<thead>
<tr>
<th>Category</th>
<th>No of Cases</th>
<th>% to total</th>
<th>Amount involved in crore</th>
<th>% to total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commercial Banks</td>
<td>169190</td>
<td>96%</td>
<td>29910.12</td>
<td>95.25%</td>
</tr>
<tr>
<td>NBFCs</td>
<td>935</td>
<td>0.53%</td>
<td>154.78</td>
<td>0.49%</td>
</tr>
<tr>
<td>UCBs</td>
<td>6345</td>
<td>3.60%</td>
<td>1057.03</td>
<td>3.37%</td>
</tr>
<tr>
<td>FIs</td>
<td>77</td>
<td>0.04%</td>
<td>279.08</td>
<td>0.89%</td>
</tr>
<tr>
<td>Total fraud cases published by RBI</td>
<td>176547</td>
<td>100.00%</td>
<td>31401.01</td>
<td>100.00%</td>
</tr>
</tbody>
</table>

OBSERVATION ON CYBER FRAUD CASES: As on 31 March, 2013 absolute cases of fraud were reported by commercial banks to the tune of 169190 and amount involved therein was Rs 29910.12 Crore while Non Banking Financial Companies (NBFCs) were reported absolute no. of cases of fraud to the tune of 935 and amount involved therein was Rs. 154.78 Crore. Similarly Urban Co-operative banks were reported absolute no. of cases of frauds to the tune 6345 and amount involved therein was Rs.1057.03 Crore while Financial Institutions (FIs) were reported absolute no. cases of fraud to the tune of 935 and amount involved therein was Rs. 154.78 Crore.

http://www.rbi.org.in
lions share and in percentage term the no of cases reported by the Commercial banks was 95.83%, Amount involved therein was to the tune of 95.25%. NBFCs, UCBs and FIs share in the No of cases was 0.53%, 3.60% and 0.04% respectively while % of amount involved was 0.49%, 3.37% and 0.89% respectively.

### A2) COMMERCIAL BANKS- FRAUD CASES & SLABWISE AMOUNT INVOLVED

**TABLE 3.24- YEAR WISE FRAUD CASES REPORTED BY COMMERCIAL BANKS**

<table>
<thead>
<tr>
<th>FY</th>
<th>Amount</th>
<th>&lt; Rs 1 lakh No. of Cases</th>
<th>&lt; Rs 1 lakh Amount Involved</th>
<th>&gt; 1 lakh and up to Rs 1 crore No. of Cases</th>
<th>&gt; 1 lakh and up to Rs 1 crore Amount Involved</th>
<th>&gt; Rs 1 cr and up to Rs 50 crore No. of Cases</th>
<th>&gt; Rs 1 cr and up to Rs 50 crore Amount Involved</th>
<th>&gt; Rs.50 crore No. of Cases</th>
<th>&gt; Rs.50 crore Amount Involved</th>
<th>Total Fraud Cases No. of Cases</th>
<th>Total Fraud Cases Amount Involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre 2004</td>
<td></td>
<td>2292</td>
<td>4.25</td>
<td>819</td>
<td>96.65</td>
<td>613</td>
<td>2951.64</td>
<td>13</td>
<td>1244.26</td>
<td>3737</td>
<td>4296.80</td>
</tr>
<tr>
<td>2004-05</td>
<td></td>
<td>7553</td>
<td>12.50</td>
<td>2407</td>
<td>287.32</td>
<td>111</td>
<td>584.89</td>
<td>1</td>
<td>53.57</td>
<td>10072</td>
<td>938.28</td>
</tr>
<tr>
<td>2005-06</td>
<td></td>
<td>11395</td>
<td>18.63</td>
<td>2334</td>
<td>290.20</td>
<td>192</td>
<td>1009.23</td>
<td>2</td>
<td>135.47</td>
<td>13923</td>
<td>1453.53</td>
</tr>
<tr>
<td>2006-07</td>
<td></td>
<td>20415</td>
<td>31.22</td>
<td>3048</td>
<td>325.02</td>
<td>158</td>
<td>791.17</td>
<td>1</td>
<td>78.45</td>
<td>23622</td>
<td>1225.86</td>
</tr>
<tr>
<td>2007-08</td>
<td></td>
<td>17691</td>
<td>30.25</td>
<td>3381</td>
<td>383.98</td>
<td>177</td>
<td>662.31</td>
<td>-</td>
<td>-</td>
<td>21249</td>
<td>1076.54</td>
</tr>
<tr>
<td>2008-09</td>
<td></td>
<td>19485</td>
<td>33.85</td>
<td>4239</td>
<td>442.94</td>
<td>214</td>
<td>1129.56</td>
<td>3</td>
<td>305.33</td>
<td>23941</td>
<td>1911.68</td>
</tr>
<tr>
<td>2009-10</td>
<td></td>
<td>20072</td>
<td>30.36</td>
<td>4494</td>
<td>474.04</td>
<td>222</td>
<td>1129.28</td>
<td>3</td>
<td>404.13</td>
<td>24791</td>
<td>2037.81</td>
</tr>
<tr>
<td>2010-11</td>
<td></td>
<td>15284</td>
<td>26.09</td>
<td>4250</td>
<td>494.64</td>
<td>277</td>
<td>1515.15</td>
<td>16</td>
<td>1796.20</td>
<td>19827</td>
<td>3832.08</td>
</tr>
<tr>
<td>2011-12</td>
<td></td>
<td>10638</td>
<td>19.05</td>
<td>3751</td>
<td>509.18</td>
<td>327</td>
<td>2113.23</td>
<td>19</td>
<td>1850.08</td>
<td>14735</td>
<td>4491.54</td>
</tr>
<tr>
<td>2012-13</td>
<td></td>
<td>9060</td>
<td>22.11</td>
<td>3816</td>
<td>491.13</td>
<td>372</td>
<td>2798.00</td>
<td>45</td>
<td>5334.76</td>
<td>13293</td>
<td>8646.00</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td>133885</td>
<td>228.31</td>
<td>32539</td>
<td>3795.10</td>
<td>2663</td>
<td>14684.46</td>
<td>103</td>
<td>11202.25</td>
<td>169190</td>
<td>29910.12</td>
</tr>
</tbody>
</table>

**OBSERVATION ON CYBER FRAUD CASES:** Fraud cases reported cumulatively by Commercial Banks as of 31/03/2004 to the tune of 3737 and amount involved therein to the tune of Rs.4296.80 crore. Whereas no. of cumulative cases reported by the Commercial Banks as of 31/03/2013 to the tune of 169190 and amount involved therein

---

436 http://www.rbi.org.in
to the tune of Rs.29910.12 Crore. During the span of nine years i.e. from 2004 to 2013
Commercial banks reported the growth in number of cases to the tune of 165493 and
growth in amount involved therein to the tune of Rs.25613.32 crore.

A) Amount less than one lakh. Under this category total 133885 fraud cases were
reported and amount involved there is was Rs. 228.11 crore. There is a tremendous
rise in the number of cases and amount involved therein from 2004-05 to
2013. Total rise in fraud cases with in the span of nine years 131593 cases
whereas there is a total rise in amount involved there in is Rs 224.06 crore.

B) Amount one lakh and above and up to one crore:- Under this category total
32539 fraud cases were reported and amount involved there is was Rs. 379.51
crore. There is a tremendous rise in the number of cases and amount involved
from 2004-05 to 2013. Total rise in fraud cases with in the span of nine years
31720 cases whereas there is a total rise in amount involved there in is Rs 3698.45
crore.

C) Amount one crore and above and up to 50 crore:- Under this category total 2663
fraud cases were reported and amount involved there is was Rs. 14684.46 crore.
There is a tremendous rise in the number of cases and amount involved from 2004-
05 to 2013. Total rise in fraud cases with in the span of nine years 2050 cases
whereas there is a total rise in amount involved there in is Rs 11732.82 crore.

D) Amount above 50 crore:- Under this category total 103 fraud cases were reported
and amount involved there is was Rs. 11202.25 crore. There is a tremendous rise
in the number of cases and amount involved therein from 2004-05 to 2013. Total
rise in fraud cases with in the span of nine years 90 cases whereas there is a total
rise in amount involved there in is Rs 9957.99 crore.
### OBSERVATION ON GROUPWISE CYBER FRAUD CASES REPORTED BY COMMERCIAL BANKS & AMOUNT INVOLVED THEREIN AS ON 31/03/2013

Total of Group wise fraud cases and amount involved

1) **Nationalised banks including SBI group** - Under this group total 29653 fraud cases was reported and amount involved therein was Rs.24828.01 crore.

2) **Private sector banks including Old & New private sector banks** - Under this Group total 93331 fraud cases and amount involved therein was Rs.3848.19 crore. Old private sector banks reported 2271 fraud cases and amount involved therein was Rs.1707.71 crore and New private sector banks reported 91060 fraud cases and amount involved therein was Rs.2140.47 crore.

3) **Foreign Banks** - Under this group total 46206 fraud cases and amount involved therein was Rs.1233.92 crore.

Reported cases of frauds under all categories were 169190 whereas amount involved therein was Rs.29910.12 crore as of 31/03/20

---

437 http://www.rbi.org.in
A-3(i) Commercial Banks-Fraud Cases & Amount involved below 1 lakh

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No of Cases</td>
<td>2292</td>
<td>7553</td>
<td>11395</td>
<td>20415</td>
<td>17691</td>
<td>19485</td>
<td>20072</td>
<td>15284</td>
<td>10638</td>
<td>9060</td>
<td>133885</td>
</tr>
<tr>
<td>(+/-)Over Previous year since 2004-05</td>
<td>-</td>
<td>3842</td>
<td>9020</td>
<td>(-2724)</td>
<td>1794</td>
<td>587</td>
<td>(-4788)</td>
<td>(-4646)</td>
<td>(-1578)</td>
<td>131593* Variation over 2004</td>
<td></td>
</tr>
<tr>
<td>% (+/-)Over Previous year since 2004-05</td>
<td>-</td>
<td>51%</td>
<td>79%</td>
<td>(-13%)</td>
<td>10%</td>
<td>3%</td>
<td>(-24%)</td>
<td>(-30%)</td>
<td>(-15%)</td>
<td>5741% Variation over 2004</td>
<td></td>
</tr>
<tr>
<td>Amount in Cr.</td>
<td>4.25</td>
<td>12.50</td>
<td>18.63</td>
<td>31.22</td>
<td>30.25</td>
<td>33.85</td>
<td>30.36</td>
<td>26.09</td>
<td>19.05</td>
<td>22.11</td>
<td>228.31</td>
</tr>
<tr>
<td>(+/-)Over Previous year since 2004-05</td>
<td>-</td>
<td>6.13</td>
<td>12.59</td>
<td>(-0.97)</td>
<td>3.60</td>
<td>3.49</td>
<td>(-4.27)</td>
<td>(-7.04)</td>
<td>(-3.06)</td>
<td>224.06* Variation over 2004</td>
<td></td>
</tr>
<tr>
<td>% (+/-)Over Previous year since 2004-05</td>
<td>-</td>
<td>49%</td>
<td>68%</td>
<td>(-0.03%)</td>
<td>12%</td>
<td>10%</td>
<td>(-14%)</td>
<td>(-27%)</td>
<td>(-16%)</td>
<td>5272% Variation over 2004</td>
<td></td>
</tr>
</tbody>
</table>

Observations on Fraud cases and amount involved below 1 lakh reported by Commercial Banks

As on 31/03/2004 number of cases of fraud below 1 lakh as reported by commercial banks was 2292. Amount involved therein was Rs.4.24 crore on the cumulative basis.

During the FY 2004-05 the number of cases under this category was 7553 as reported by commercial banks and amount involved there in was Rs.12.50 crore. During the FY 2005-06 there was a growth of 9020 fraud cases with 79% rise over the previous year and there was a growth of Rs. 6.13 crore with 49% rise in amount involved in fraud cases over the previous year. During the FY 2006-07 there was growth of 9020 fraud cases with 79% rise over the previous year and a growth of Rs. 6.13 crore with 49% rise in amount involved in fraud cases over the previous year. During the FY 2007-08 there was a fall of 2724 fraud cases with 79% decrease over the previous year and a fall of Rs. 0.97 crore with 3% fall in the amount involved in fraud cases over the previous year. During FY 2008-09, there was again growth of 1794 cases with 10% rise over the previous year and a growth of Rs. 3.60 crore with 12% rise in amount involved in fraud cases over the previous year. During FY 2009-10, there was again a growth of 587 cases with 3% rise over the previous year and a growth of Rs. 3.49 crore with 10% rise.
in the amount involved in fraud cases over the previous year. During the FY 2010-11, there was a fall of 4788 fraud cases with 24% decrease over the previous year and a fall of Rs. 4.27 crore with 14% fall in the amount involved in fraud cases over the previous year. During the FY 2011-12, there was a fall of 4646 fraud cases with 30% decrease over the previous year and a fall of Rs. 7.04 crore with 27% fall in amount involved in fraud cases over the previous year. During the FY 2012-13, there was a fall of 1578 fraud cases with 15% decrease over the previous year and a fall of Rs. 3.06 crore with 16% fall in amount involved in fraud cases over the previous year.

As on 31/03/2013 there is a variation of 131593 cases over 31/03/2004 with 5741% and growth of Rs. 224.06 crore with 5272% growth in amount involved over the previous year.

**A-3(ii) Commercial Banks- Fraud Cases and Amount Involved (Above 1lakh & Upto 1crore)**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No of Cases</td>
<td>819</td>
<td>2407</td>
<td>2334</td>
<td>3048</td>
<td>3381</td>
<td>4239</td>
<td>4494</td>
<td>4250</td>
<td>3751</td>
<td>3816</td>
<td>32539</td>
</tr>
<tr>
<td>(+/-)Over Previous year since 2004-05</td>
<td>-</td>
<td>-</td>
<td>(-)73</td>
<td>714</td>
<td>333</td>
<td>858</td>
<td>255</td>
<td>(-)244</td>
<td>(-)499</td>
<td>65</td>
<td>31785 Variation over2004</td>
</tr>
<tr>
<td>% (+/-)Over Previous year since 2004-05</td>
<td>-</td>
<td>-</td>
<td>(-)3%</td>
<td>31%</td>
<td>11%</td>
<td>25%</td>
<td>6%</td>
<td>(-)5%</td>
<td>(-)12%</td>
<td>2%</td>
<td>3881% Variation over2004</td>
</tr>
<tr>
<td>Amount in Cr.</td>
<td>96.6</td>
<td>287.32</td>
<td>290.20</td>
<td>325.02</td>
<td>383.98</td>
<td>442.94</td>
<td>474.04</td>
<td>494.64</td>
<td>509.18</td>
<td>491.13</td>
<td>3795.10</td>
</tr>
<tr>
<td>(+/-)Over Previous year since 2004-05</td>
<td>-</td>
<td>-</td>
<td>2.88</td>
<td>34.82</td>
<td>58.96</td>
<td>58.96</td>
<td>31.10</td>
<td>20.60</td>
<td>14.54</td>
<td>(-)18.05</td>
<td>3698.45 Variation over2004</td>
</tr>
<tr>
<td>% (+/-)Over Previous year since 2004-05</td>
<td>-</td>
<td>-</td>
<td>1%</td>
<td>12%</td>
<td>18%</td>
<td>15%</td>
<td>7%</td>
<td>4%</td>
<td>3%</td>
<td>(-)4%</td>
<td>38% Variation over2004</td>
</tr>
</tbody>
</table>
Observations on year wise fraud cases and amount involved above 1 lakh & up to 1 crore reported by Commercial Banks

As on 31/03/2004, the number of cases of fraud above 1 lakh and up to Rs. 1 crore as reported by commercial banks was 819 and the amount involved therein was Rs. 96.65 crore on the cumulative basis.

During the FY 2004-05, the number of cases under this category was 2407 as reported by commercial banks and the amount involved there in was Rs. 287.32 crore.

During the FY 2005-06, there was a fall of 73 fraud cases with 3% fall over the previous year and there was a growth of Rs. 2.88 crore with 1% rise in amount involved in fraud cases over the previous year.

During the FY 2006-07, there was growth of 714 fraud cases with 31% rise over the previous year and a growth of Rs. 34.82 crore with 12% rise in amount involved in fraud cases over the previous year.

During the FY 2007-08, there was a growth of 333 fraud cases with 11% increase over the previous year and a growth of Rs. 58.96 crore with 18% increase in the amount involved in fraud cases over the previous year.

During FY 2008-09, there was again growth of 858 cases with 25% rise over the previous year and a growth of Rs. 58.96 crore with 15% rise in amount involved in fraud cases over the previous year.

During FY 2009-10, there was again a growth of 255 cases with 6% rise over the previous year and a growth of Rs. 31.10 crore with 7% rise in the amount involved in fraud cases over the previous year.

During the FY 2010-11, there was a fall of 244 fraud cases with 5% decrease over the previous year and a growth of Rs. 20.60 crore with 4% rise in the amount involved in fraud cases over the previous year.

During the FY 2011-12, there was a fall of 499 fraud cases with 12% decrease over the previous year and a growth of Rs. 14.54 crore with 3% rise in amount involved in fraud cases over the previous year.

During the FY 2012-13, there was a growth of 65 fraud cases with 2% rise over the previous year and a fall of Rs. 18.05 crore with 4% fall in amount involved in fraud...
cases over the previous year. As on 31/03/2013 there is a variation of 31785 cases over 31/03/2004 with 3881% and growth of Rs. 3698.45 crore with 38% growth in amount involved over the previous year.

**A-3(iii) Commercial Banks- Amount Involved In Frauds(1 crore and above)**

**Table 3.28-Commercial Banks- Amount involved in Fraud Cases (1 Crore and above)**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No of Cases</td>
<td>626</td>
<td>112</td>
<td>194</td>
<td>159</td>
<td>177</td>
<td>217</td>
<td>225</td>
<td>293</td>
<td>346</td>
<td>417</td>
<td>2766</td>
</tr>
<tr>
<td>(+/-) Over Previous year since 2004-05</td>
<td>-</td>
<td>-</td>
<td>82</td>
<td>(-35)</td>
<td>18</td>
<td>23</td>
<td>8</td>
<td>68</td>
<td>53</td>
<td>71</td>
<td>2140 Variation over 2004</td>
</tr>
<tr>
<td>% (+/-) Over Previous year since 2004-05</td>
<td>-</td>
<td>-</td>
<td>73%</td>
<td>(-18%)</td>
<td>11%</td>
<td>13%</td>
<td>4%</td>
<td>30%</td>
<td>18%</td>
<td>21%</td>
<td>342% Variation over 2004</td>
</tr>
<tr>
<td>Amount in Cr.</td>
<td>4195.90</td>
<td>638.46</td>
<td>1144.70</td>
<td>869.62</td>
<td>662.31</td>
<td>1434.89</td>
<td>1533.41</td>
<td>3311.35</td>
<td>3963.31</td>
<td>8132.76</td>
<td>25886.71</td>
</tr>
<tr>
<td>(+/-) Over Previous year since 2004-05</td>
<td>-</td>
<td>506.24</td>
<td>(-275.08)</td>
<td>(-206.69)</td>
<td>(772.58)</td>
<td>98.52</td>
<td>1777.94</td>
<td>651.96</td>
<td>4169.45</td>
<td>21690.81</td>
<td>517% Variation over 2004</td>
</tr>
<tr>
<td>% (+/-) Over Previous year since 2004-05</td>
<td>-</td>
<td>79%</td>
<td>(-24%)</td>
<td>(-24%)</td>
<td>117%</td>
<td>13%</td>
<td>116%</td>
<td>20%</td>
<td>105%</td>
<td>517%</td>
<td></td>
</tr>
</tbody>
</table>

**Observation on year wise fraud cases and amount involved 1 crore and above**

As on 31/03/2004 number of cases of fraud above 1 crore as reported by commercial banks was 626 and amount involved therein was Rs.4195.90 crore on the cumulative basis.

During the FY 2004-05 the number of cases under this category was 112 as reported by commercial banks and amount involved there in was Rs.638.46 crore.

During the FY 2005-06 there was a growth of 82 fraud cases with 73% increase over the previous year and there was a growth of Rs. 506.24 crore with 79% rise in amount involved in fraud cases over the previous year.
During the FY 2006-07, there was a fall of 35 fraud cases with 18% decrease over the previous year and a fall of Rs. 506.24 crore with 24% decrease in amount involved in fraud cases over the previous year.

During the FY 2007-08, there was a growth of 18 fraud cases with 11% increase over the previous year and a fall of Rs. 206.69 crore with 24% increase in the amount involved in fraud cases over the previous year.

During FY 2008-09, there was a growth of 23 cases with 13% rise over the previous year and a growth of Rs. 772.58 crore with 117% rise in amount involved in fraud cases over the previous year.

During FY 2009-10, there was again a growth of 8 cases with 4% rise over the previous year and a growth of Rs. 98.52 crore with 13% rise in the amount involved in fraud cases over the previous year.

During the FY 2010-11, there was a growth of 68 fraud cases with 30% increase over the previous year and a growth of Rs. 1777.94 crore with 116% rise in the amount involved in fraud cases over the previous year.

During the FY 2011-12, there was a growth of 53 fraud cases with 18% increase over the previous year and a growth of Rs. 651.96 crore with 20% rise in amount involved in fraud cases over the previous year.

During the FY 2012-13, there was a growth of 71 fraud cases with 21% rise over the previous year and a growth of Rs. 4169.45 crore with 105% rise in amount involved in fraud cases over the previous year.

As on 31/03/2013, there is a variation of 2140 cases over 31/03/2004 with 342% and growth of Rs. 21690.81 crore with 517% growth in amount over the previous year. It is observed from the above that the cyber legislation and other existing laws related to e-banking operation in India are not adequate and sufficient to control the mounting cyber crime. Therefore, the number of incidents showing the rising trend during last 9 years i.e. from 2004 to 2013. Therefore it gives the impression that there is no adequate and sufficient legal control of cyber crimes against e-banking in India and for this reason the numbers of cyber crime incidents are enormously increased.

*****
3.4.3(I) 4. BANK GROUPWISE CATEGORIES OF FRAUDS

There are three main categories of frauds are classified as

A. KYC related frauds (Know Your Customer)
B. Advances related frauds
C. Technology related frauds

4A) KYC RELATED FRAUDS

KYC related frauds are mainly committed in deposit accounts. These frauds generally related to money laundering cases where fake identity is used by the miscreants. These frauds are included in technology related frauds. It reveals from the close examination of the reported fraud cases that around 65% of the total fraud cases reported by banks were technology related frauds. These frauds covers are committed through internet banking channel, ATMs and other alternate payment channels like credit/ debit/prepaid cards. These frauds are committed on electronic banking channels as described above. These frauds are included in technology related frauds hence separately not discussed

4B) ADVANCES RELATED FRAUDS (RS. 1 CRORE & ABOVE)

A closer examination of the reported fraud cases has revealed that around 65% of the total fraud cases reported by banks were technology related frauds while the advances portfolio accounted for a major proportion (64%) of the total amount involved in frauds. Table 4 below shows that relatively large value advances related frauds (> Rs. 1 crore) have increased both in terms of number and amount involved over the last few years. These frauds are advances related frauds and the miscreants are committed these frauds to dupe the bank funds. These frauds are not the part of cyber crimes hence these frauds hence separately not discussed

4C) BANK GROUP WISE TECHNOLOGY RELATED FRAUDS

There has been a remarkable shift in the service delivery by the banks with greater combination of technology in the financial services sector in general and in banking sector in particular. There have been a number of instances of banking frauds of low value wherein the criminals have used hostile software programs or malware attacks, phishing, Vishing (voicemail), SMSishing (text messages) and other advanced techniques excluding stealing confidential data to commit frauds
4C) BANK GROUP WISE TECHNOLOGY RELATED FRAUDS

Table 3.29 Bank Group wise Technology Related Frauds

<table>
<thead>
<tr>
<th>Bank Group</th>
<th>Total up to 31/03/2008</th>
<th>Total of 4 years (2009-10 to 2012-13)</th>
<th>Cumulative Total (As on 31/03/2013)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No. of Cases</td>
<td>Amount Involved</td>
<td>No. of Cases</td>
</tr>
<tr>
<td>A) Nationalised Banks including SBI Group</td>
<td>201</td>
<td>3.28</td>
<td>623</td>
</tr>
<tr>
<td>i) Old Private Sector Banks</td>
<td>27</td>
<td>0.54</td>
<td>28</td>
</tr>
<tr>
<td>ii) New Private Sector Banks</td>
<td>40336</td>
<td>77.03</td>
<td>33985</td>
</tr>
<tr>
<td>B) Private Sector Banks (SUBTOTAL)</td>
<td>41187</td>
<td>103.17</td>
<td>34013</td>
</tr>
<tr>
<td>C) Foreign Banks</td>
<td>18220</td>
<td>67.25</td>
<td>18235</td>
</tr>
<tr>
<td>Grand Total</td>
<td>59608</td>
<td>173.70</td>
<td>52871</td>
</tr>
</tbody>
</table>

OBSERVATIONS ON GROUPWISE TECHNOLOGY RELATED FRAUDS

The above table shows that relatively large value advances related frauds i.e. above Rs. 1 crore have been increased both in terms of number and amount involved over the years in general and over the last four years in particular. The advances portfolio accounted for a major proportion (64%) of the total amount involved in frauds. No of cases relating to high value frauds reported by the Commercial Banks in India comprising of All Nationalised Banks Including State Bank Group, All Private Sector Banks including Old & New and Foreign Banks during the period 2009-10 to 2012-13 depicts the increasing trends. As on 31/03/2013 there are 112479 fraud cases reported by All commercial Banks in India on cumulative basis. Amount involved in the technology related frauds reported by the by the Commercial Banks in India during the period 2009-10 to 2012-13 also depicts the increasing trends. As on 31/03/2013, total amount Rs.382.93 crore was reported by All Commercial Banks in India involved in the fraud cases cumulatively.

The number of technology related incidents of frauds depicts the rising trend during last 9 years i.e. from 2004 to 2013 in the cyber crime incidents. The reason for rising in advances related frauds in the banking industry is due to insufficient and inadequate cyber laws and failed to control the rising incidences of cyber crimes in banking sector.

438 http://www.rbi.org.in
3.4.3(J) 5) CYBER FRAUDS IN PUBLIC SECTOR BANKS

The Minister of State for Finance, Shri Namo Narian Meena in a written reply to the unstarred question No.2398 in the Rajya Sabha answered on the March 19, 2013 that The Reserve Bank of India has informed that the incidents of frauds reported by Public Sector Banks with amount involved for the last three Financial Years is as under:

5A) YEAR WISE CYBER FRAUDS CASES IN PUBLIC SECTOR BANKS (FY2010-13)

Table 3.30 - Yearwise Cyber Frauds Cases in Public Sector Banks (FY2009-10 to FY2012-13)

<table>
<thead>
<tr>
<th>S.N.</th>
<th>Financial Year</th>
<th>No. of frauds cases reported</th>
<th>Amount involved in lacs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>2009-10</td>
<td>3363</td>
<td>161268.15</td>
</tr>
<tr>
<td>2.</td>
<td>2010-11</td>
<td>3718</td>
<td>256900.48</td>
</tr>
<tr>
<td>3.</td>
<td>2011-12</td>
<td>3392</td>
<td>402532.04</td>
</tr>
<tr>
<td>4.</td>
<td>2012-13 (up to Dec 2012)</td>
<td>2543</td>
<td>657391.40</td>
</tr>
</tbody>
</table>

*Bank wise details of Cyber Frauds for the last 4 years is at Annexure – 1.

OBSERVATIONS ON YEARWISE CYBER FRAUDS IN PUBLIC SECTOR BANKS

During the FY 2009-10 fraud cases reported to the tune of 3363 and amount involved there in was Rs.161268.15 lakh. During the FY 2010-11 there was a rise in the fraud cases over the previous year and recorded 3718 cases and amount involved therein was Rs.256900.48 lakh. During FY 2011-12 there is a decline trend in reported cases but increasing trend in amount involved over the previous year. The cases reported during the year were 3392 and amount involved there in was Rs.402532.04 lakh. During the year 2012-13 the reported cases were 2543 and amount involved there in was Rs.657391.40 lakh.

---

439 Rajya Sabha Unstarred Question No. 2398 answered On the March 19, 2013 by Namo Narayan Meena State Finance Minister
## Table 3.31 - Cyber Fraud Cases in Nationalised Banks (FY 2009-2012) Annexure - I.

<table>
<thead>
<tr>
<th>S.N.</th>
<th>Bank Name</th>
<th>FY2009-10 No. of Cases</th>
<th>FY2009-10 Amount Involved</th>
<th>FY2010-11 No. of Cases</th>
<th>FY2010-11 Amount Involved</th>
<th>FY2011-12 No. of Cases</th>
<th>FY2011-12 Amount Involved</th>
<th>FY2012-13 No. of Cases</th>
<th>FY2012-13 Amount Involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Allahabad Bank</td>
<td>112</td>
<td>2371.25</td>
<td>110</td>
<td>4025.51</td>
<td>106</td>
<td>12121.30</td>
<td>116</td>
<td>30384.20</td>
</tr>
<tr>
<td>2.</td>
<td>Andhra Bank</td>
<td>95</td>
<td>7001.75</td>
<td>59</td>
<td>2471.05</td>
<td>97</td>
<td>6901.84</td>
<td>63</td>
<td>11361.67</td>
</tr>
<tr>
<td>3.</td>
<td>Bank of Baroda</td>
<td>233</td>
<td>3764.96</td>
<td>251</td>
<td>5726.72</td>
<td>184</td>
<td>5730.55</td>
<td>91</td>
<td>42376.19</td>
</tr>
<tr>
<td>4.</td>
<td>Bank of India</td>
<td>221</td>
<td>5790.15</td>
<td>249</td>
<td>11683.37</td>
<td>228</td>
<td>50261.80</td>
<td>304</td>
<td>51589.54</td>
</tr>
<tr>
<td>5.</td>
<td>Bank of Maharashtra</td>
<td>81</td>
<td>1847.43</td>
<td>95</td>
<td>6529.75</td>
<td>55</td>
<td>1327.45</td>
<td>33</td>
<td>3852.13</td>
</tr>
<tr>
<td>6.</td>
<td>Canara Bank</td>
<td>151</td>
<td>6210.67</td>
<td>118</td>
<td>12243.09</td>
<td>125</td>
<td>38683.77</td>
<td>55</td>
<td>19498.90</td>
</tr>
<tr>
<td>7.</td>
<td>Central Bank of India</td>
<td>165</td>
<td>8369.19</td>
<td>135</td>
<td>30883.05</td>
<td>117</td>
<td>3333.92</td>
<td>92</td>
<td>12852.43</td>
</tr>
<tr>
<td>8.</td>
<td>Corporation Bank</td>
<td>87</td>
<td>1091.08</td>
<td>83</td>
<td>7548.27</td>
<td>107</td>
<td>5705.32</td>
<td>100</td>
<td>13608.29</td>
</tr>
<tr>
<td>9.</td>
<td>Dena Bank</td>
<td>35</td>
<td>980.55</td>
<td>42</td>
<td>707.83</td>
<td>38</td>
<td>4951.94</td>
<td>23</td>
<td>21649.53</td>
</tr>
<tr>
<td>10.</td>
<td>IDBI Bank Limited</td>
<td>121</td>
<td>22126.00</td>
<td>137</td>
<td>27590.38</td>
<td>266</td>
<td>11188.95</td>
<td>132</td>
<td>3719.99</td>
</tr>
<tr>
<td>11.</td>
<td>Indian Bank</td>
<td>99</td>
<td>6250.15</td>
<td>104</td>
<td>3858.89</td>
<td>94</td>
<td>5793.67</td>
<td>75</td>
<td>15194.17</td>
</tr>
<tr>
<td>12.</td>
<td>Indian Overseas Bank</td>
<td>134</td>
<td>10803.90</td>
<td>115</td>
<td>38948.59</td>
<td>134</td>
<td>51903.01</td>
<td>110</td>
<td>46003.58</td>
</tr>
<tr>
<td>13.</td>
<td>Oriental Bank of Commerce</td>
<td>54</td>
<td>1133.46</td>
<td>89</td>
<td>11983.30</td>
<td>77</td>
<td>22702.74</td>
<td>44</td>
<td>14027.50</td>
</tr>
<tr>
<td>14.</td>
<td>Punjab &amp; Sind Bank</td>
<td>33</td>
<td>2855.52</td>
<td>37</td>
<td>740.15</td>
<td>23</td>
<td>4110.91</td>
<td>24</td>
<td>6691.59</td>
</tr>
<tr>
<td>15.</td>
<td>Punjab National Bank</td>
<td>244</td>
<td>7620.35</td>
<td>358</td>
<td>9856.84</td>
<td>281</td>
<td>19561.85</td>
<td>247</td>
<td>65146.04</td>
</tr>
<tr>
<td>16.</td>
<td>Syndicate Bank</td>
<td>200</td>
<td>5489.24</td>
<td>147</td>
<td>5847.77</td>
<td>117</td>
<td>3491.42</td>
<td>127</td>
<td>20266.80</td>
</tr>
<tr>
<td>17.</td>
<td>UCO Bank</td>
<td>133</td>
<td>2968.08</td>
<td>247</td>
<td>13937.51</td>
<td>161</td>
<td>10286.46</td>
<td>62</td>
<td>34951.06</td>
</tr>
<tr>
<td>18.</td>
<td>Union Bank of India</td>
<td>137</td>
<td>22433.80</td>
<td>141</td>
<td>5353.19</td>
<td>90</td>
<td>12546.03</td>
<td>101</td>
<td>69263.10</td>
</tr>
<tr>
<td>19.</td>
<td>United Bank of India</td>
<td>60</td>
<td>2085.01</td>
<td>95</td>
<td>3111.60</td>
<td>116</td>
<td>21364.44</td>
<td>151</td>
<td>13295.27</td>
</tr>
<tr>
<td><strong>Nationalised Banks</strong></td>
<td><strong>2564</strong></td>
<td><strong>125162.88</strong></td>
<td><strong>2683</strong></td>
<td><strong>206179.45</strong></td>
<td><strong>2483</strong></td>
<td><strong>307486.97</strong></td>
<td><strong>1981</strong></td>
<td><strong>536165.90</strong></td>
<td></td>
</tr>
</tbody>
</table>
OBSEVATIONS ON BANKWISE CYBER FRAUDS IN PUBLIC SECTOR BANKS

During the FY 2009-10 total fraud cases reported to the tune of 3363 in Nationalised Banks Group and amount involved there in was Rs.125162.88lakh while in State Bank Group total 799 fraud cases reported and amount involved there in was reported to the tune of Rs.36105.27 lakh. Total 3363 cyber fraud cases reported in Public Sector Banks Group and amount involved there in was Rs.161268.15 lakh. During the FY 2010-11, in Nationalised Banks there is rise in the fraud cases over the previous year and recorded 2683 cases and amount involved therein was Rs. 206179.45 lakh while in State Bank Group total 1035 fraud cases reported and amount involved there in was reported to the tune of Rs.50721.03 lakh. Total 3718 cyber fraud cases reported in the Public Sector Bank Group and amount involved there in was Rs.256900.48 lakh. During FY 2011-12 in Nationalised Banks Group there is a rising trend in reported cases and also the increasing trend in amount involved over the previous year while in State Bank Group there is a declining trend in reported cases and increasing trend in amount involved over the previous year. In public Sector Banks there is a declining trend in reported cases and also the increasing trend in amount involved over the previous year. The cases reported during the year in Nationalised Banks were 2483 and amount involved there in was Rs.307486.97 lakh while in State Bank Group total 909 fraud cases
reported and amount involved there in was reported to the tune of Rs.95045.07 lakh. Total 3392 cyber fraud cases reported in the Public Sector Bank Group and amount involved there in was Rs.402532.04 lakh. During the FY 2012-13 the reported cases of Cyber Fraud cases up to 31/12/2012 in Nationalised Banks were to the tune of 1981 cases and amount involved there in was Rs. 536165.90 lakh while in State Bank Group total 562 fraud cases reported and amount involved there in was reported to the tune of Rs.121225.50 lakh. Total 2543 cyber fraud cases reported in the Public Sector Bank Group and amount involved there in was Rs. 657391.40 lakh. The number of cases and amount involved in fraud cases is showing an increasing trend. The reason for rising in the advances related frauds in the banking industry is due to insufficient and inadequate cyber laws and failed to control the rising incidences of cyber crimes in the banking sector.

3.4.3(K) 6) CYBER FRAUDS IN SCHEDULED COMMERCIAL BANKS

The Minister of State for Finance, Shri Namo Narian Meena in a written reply to a question in the Lok Sabha on 22\textsuperscript{nd} February 2013 replied in the following manner\textsuperscript{440} The details furnished by Reserve Bank of India (RBI) in respect of Scheduled Commercial Banks pertaining to frauds relating to ATMs/Debit Cards/ Internet Banking and Credit Cards is as under:\textsuperscript{441}

6A) YEARWISE CYBER FRAUDS IN SCHEDULED COMMERCIAL BANKS

Table3.32- Year wise Cyber Frauds in Scheduled Commercial Banks (2009-2012) (Amt. in Lakh)\textsuperscript{442}

<table>
<thead>
<tr>
<th>S.N</th>
<th>Calendar Year</th>
<th>Total Cases Reported</th>
<th>Amount Involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2009</td>
<td>21966</td>
<td>7233.31</td>
</tr>
<tr>
<td>2</td>
<td>2010</td>
<td>15018</td>
<td>4048.94</td>
</tr>
<tr>
<td>3</td>
<td>2011</td>
<td>9588</td>
<td>3672.19</td>
</tr>
<tr>
<td>4</td>
<td>2012</td>
<td>8322</td>
<td>5266.95</td>
</tr>
</tbody>
</table>

*Bank wise details of Cyber Crimes for the last 4 years is at Annexure – 1.

A-5) OBSERVATIONS ON CYBER FRAUDS IN SCHEDULED COMMERCIAL BANKS

During the Calendar Year 2009-10 fraud cases reported to the tune of 21966 and amount involved there in was Rs.7233.31 lakh. During the Calendar Year 2010-11 there was a rise in the fraud cases over the previous year and recorded 15018 cases

\textsuperscript{440} Press Information Bureau of India Ministry of Finance published the news on 26\textsuperscript{th} February 2013

\textsuperscript{441} Details of Calendar Year wise Cyber Frauds in Banks, Retrieved from www.rbi.org.in (2013)

\textsuperscript{442} Lok Sabha Unstarred Question No. 2398 answered On the March 19, 2013 by Namo Narayan Meena State Finance Minister
and amount involved therein was Rs. 4048.94 lakh. During Calendar Year 2011-12 it shows a decline trend in reported cases and also in amount involved in cyber frauds in Commercial Banks over the previous year. The cases reported during the calendar year were 9588 and amount involved there in was Rs.3672.19 lakh. During the year 2012-13 the reported cases were 8322 and amount involved there in was Rs.5266.95 lakh. The number of cases and amount involved in fraud cases is showing an increasing trend in Nationalised Banks and State Bank Group both in terms of incidents of fraud cases and amount involved there in. The Private Sector Banks & Foreign Banks though recorded the negative growth in number of fraud cases and amount involved but the reported cases volume is so enormous which caused the concern and the situation in Private Sector Banks and Foreign Banks is alarming. In short, the rising incidences of frauds in the banking industry are due to insufficient and inadequate cyber laws and these legislations are not efficient to control the cyber crimes against e-banking in India.

6B) YEARWISE CYBER FRAUD CASES IN COMMERCIAL BANKS (2009-2012)  

Table 3.33-Bankwise Cyber Fraud Cases in Commercial Banks (2009-2012)(Amt.in lakh) Annexure-I.

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Bank Name</th>
<th>Calendar Year 2009</th>
<th>Calendar Year 2010</th>
<th>Calendar Year 2011</th>
<th>Calendar Year 2012</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>No. of Cases</td>
<td>Amount Involved</td>
<td>No. of Cases</td>
<td>Amount Involved</td>
</tr>
<tr>
<td>1.</td>
<td>Allahabad Bank</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>2.</td>
<td>American Express Banking Corporation</td>
<td>980</td>
<td>904.57</td>
<td>819</td>
<td>360.75</td>
</tr>
<tr>
<td>3.</td>
<td>Andhra Bank</td>
<td>0</td>
<td>0.00</td>
<td>1</td>
<td>31.85</td>
</tr>
<tr>
<td>4.</td>
<td>Axis Bank Ltd.</td>
<td>20</td>
<td>110.58</td>
<td>14</td>
<td>44.59</td>
</tr>
<tr>
<td>5.</td>
<td>Bank of Baroda</td>
<td>6</td>
<td>6.88</td>
<td>5</td>
<td>12.40</td>
</tr>
<tr>
<td>6.</td>
<td>Bank of India</td>
<td>5</td>
<td>5.21</td>
<td>2</td>
<td>14.61</td>
</tr>
<tr>
<td>7.</td>
<td>Bank of Maharashtra</td>
<td>4</td>
<td>3.55</td>
<td>4</td>
<td>4.69</td>
</tr>
<tr>
<td>8.</td>
<td>Bank of Rajasthan Ltd (Merged With ICICI)</td>
<td>0</td>
<td>0.00</td>
<td>1</td>
<td>0.31</td>
</tr>
<tr>
<td>10.</td>
<td>Canara Bank</td>
<td>6</td>
<td>1.39</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>11.</td>
<td>Central Bank of India</td>
<td>2</td>
<td>0.84</td>
<td>2</td>
<td>2.15</td>
</tr>
<tr>
<td>12.</td>
<td>Citi Bank N.A.</td>
<td>1226</td>
<td>773.18</td>
<td>925</td>
<td>521.27</td>
</tr>
<tr>
<td>13.</td>
<td>Corporation Bank</td>
<td>2</td>
<td>0.72</td>
<td>2</td>
<td>6.21</td>
</tr>
<tr>
<td>14.</td>
<td>Dena Bank</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>15.</td>
<td>Deutsche Bank (Asia)</td>
<td>61</td>
<td>116.64</td>
<td>35</td>
<td>81.94</td>
</tr>
<tr>
<td>16.</td>
<td>Development Credit Bank</td>
<td>2</td>
<td>0.96</td>
<td>2</td>
<td>0.30</td>
</tr>
</tbody>
</table>

443 Lok Sabha Unstarred Question No. 2398 answered On the March 19, 2013 by Namo Narayan Meena State Finance Minister (Annexure-1)
<table>
<thead>
<tr>
<th></th>
<th>Bank Name</th>
<th>No. of Branches</th>
<th>Total Branches</th>
<th>No. of ATMs</th>
<th>Total ATMs</th>
<th>No. of POs</th>
<th>Total POs</th>
<th>No. of POS terminals</th>
<th>Total POS terminals</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>Dhanlaxmi Bank Ltd.</td>
<td>0</td>
<td>0.00</td>
<td>3</td>
<td>2.29</td>
<td>1</td>
<td>3.02</td>
<td>4</td>
<td>1.09</td>
</tr>
<tr>
<td>18</td>
<td>Federal Bank Limited</td>
<td>0</td>
<td>0.00</td>
<td>2</td>
<td>20.50</td>
<td>0</td>
<td>0.00</td>
<td>3</td>
<td>83.69</td>
</tr>
<tr>
<td>19</td>
<td>Firststrand Bank</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
<td>14</td>
<td>4.82</td>
</tr>
<tr>
<td>20</td>
<td>HDFC Bank Ltd.</td>
<td>211</td>
<td>165.58</td>
<td>208</td>
<td>125.98</td>
<td>386</td>
<td>276.68</td>
<td>525</td>
<td>409.56</td>
</tr>
<tr>
<td>21</td>
<td>Hongkong &amp; Shanghai Banking Corp. Ltd</td>
<td>3093</td>
<td>722.45</td>
<td>2520</td>
<td>293.02</td>
<td>793</td>
<td>181.41</td>
<td>709</td>
<td>180.73</td>
</tr>
<tr>
<td>22</td>
<td>ICICI Bank Ltd.</td>
<td>15666</td>
<td>3731.95</td>
<td>9811</td>
<td>1920.28</td>
<td>6013</td>
<td>1096.6</td>
<td>3428</td>
<td>676.51</td>
</tr>
<tr>
<td>23</td>
<td>Indian Bank</td>
<td>24</td>
<td>16.29</td>
<td>13</td>
<td>15.29</td>
<td>3</td>
<td>44.64</td>
<td>87</td>
<td>203.04</td>
</tr>
<tr>
<td>24</td>
<td>Indian Overseas Bank</td>
<td>2</td>
<td>0.39</td>
<td>3</td>
<td>1.44</td>
<td>10</td>
<td>176.03</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>25</td>
<td>IndsInd Bank Ltd.</td>
<td>0</td>
<td>0.00</td>
<td>3</td>
<td>7.59</td>
<td>3</td>
<td>1.19</td>
<td>2</td>
<td>4.61</td>
</tr>
<tr>
<td>26</td>
<td>Jammu &amp; Kashmir Bank</td>
<td>1</td>
<td>4.51</td>
<td>2</td>
<td>6.58</td>
<td>0</td>
<td>0.00</td>
<td>1</td>
<td>13.88</td>
</tr>
<tr>
<td>27</td>
<td>Karur Vysya Bank Ltd.</td>
<td>0</td>
<td>0.00</td>
<td>1</td>
<td>23.14</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>28</td>
<td>Kotak Mahindra Bank Ltd.</td>
<td>57</td>
<td>75.26</td>
<td>31</td>
<td>29.63</td>
<td>52</td>
<td>33.11</td>
<td>78</td>
<td>67.64</td>
</tr>
<tr>
<td>29</td>
<td>Laxmi Vilas Bank Ltd</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
<td>1</td>
<td>10.00</td>
</tr>
<tr>
<td>30</td>
<td>Oriental Bank of Comm.</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>4.75</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>31</td>
<td>Punjab National Bank</td>
<td>33</td>
<td>50.15</td>
<td>108</td>
<td>248.64</td>
<td>28</td>
<td>170.19</td>
<td>14</td>
<td>99.43</td>
</tr>
<tr>
<td>32</td>
<td>South Indian Bank Ltd.</td>
<td>1</td>
<td>2.47</td>
<td>1</td>
<td>0.54</td>
<td>2</td>
<td>0.84</td>
<td>2</td>
<td>0.49</td>
</tr>
<tr>
<td>33</td>
<td>Standard Chartered Bank</td>
<td>374</td>
<td>356.37</td>
<td>386</td>
<td>187.52</td>
<td>435</td>
<td>185.11</td>
<td>511</td>
<td>207.96</td>
</tr>
<tr>
<td>34</td>
<td>State Bank of India</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
<td>2</td>
<td>14.62</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>35</td>
<td>State Bank of Bikaner &amp;Jaipur</td>
<td>2</td>
<td>6.66</td>
<td>2</td>
<td>0.15</td>
<td>2</td>
<td>3.49</td>
<td>1</td>
<td>49.32</td>
</tr>
<tr>
<td>36</td>
<td>State Bank of Hyderabad</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
<td>4</td>
<td>63.33</td>
<td>6</td>
<td>50.52</td>
</tr>
<tr>
<td>37</td>
<td>State Bank of Indore ( Merged with SBI)</td>
<td>1</td>
<td>0.80</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>38</td>
<td>State Bank of Mysore</td>
<td>0</td>
<td>0.00</td>
<td>1</td>
<td>1.01</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>39</td>
<td>State Bank of Patiala</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
<td>4</td>
<td>80.45</td>
<td>2</td>
<td>31.42</td>
</tr>
<tr>
<td>40</td>
<td>State Bank of Patiala</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
<td>6</td>
<td>10.30</td>
<td>3</td>
<td>3.20</td>
</tr>
<tr>
<td>41</td>
<td>State Bank of Travancore</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
<td>2</td>
<td>1.60</td>
<td>2</td>
<td>31.22</td>
</tr>
<tr>
<td>42</td>
<td>Syndicate Bank</td>
<td>2</td>
<td>0.53</td>
<td>1</td>
<td>2.32</td>
<td>1</td>
<td>0.56</td>
<td>2</td>
<td>7.87</td>
</tr>
<tr>
<td>43</td>
<td>Tamilnad Mercantile Bank</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
<td>1</td>
<td>0.27</td>
<td>1</td>
<td>1.49</td>
</tr>
<tr>
<td>44</td>
<td>The Royal Bank Of Scotland</td>
<td>142</td>
<td>141.30</td>
<td>51</td>
<td>44.52</td>
<td>46</td>
<td>49.35</td>
<td>14</td>
<td>12.10</td>
</tr>
<tr>
<td>45</td>
<td>UCO Bank</td>
<td>2</td>
<td>0.58</td>
<td>1</td>
<td>1.60</td>
<td>0</td>
<td>0.00</td>
<td>4</td>
<td>31.22</td>
</tr>
<tr>
<td>46</td>
<td>Union Bank of India</td>
<td>5</td>
<td>10.45</td>
<td>7</td>
<td>19.22</td>
<td>2</td>
<td>7.86</td>
<td>9</td>
<td>70.17</td>
</tr>
<tr>
<td>47</td>
<td>United Bank of India</td>
<td>1</td>
<td>1.37</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
<td>6</td>
<td>32.86</td>
</tr>
<tr>
<td>48</td>
<td>Vijaya Bank</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
<td>1</td>
<td>8.40</td>
</tr>
<tr>
<td></td>
<td>GRAND TOTAL</td>
<td>21966</td>
<td>7233.31</td>
<td>15018</td>
<td>4048.94</td>
<td>9588</td>
<td>3672.19</td>
<td>8322</td>
<td>5266.95</td>
</tr>
</tbody>
</table>
A-6) OBSERVATIONS ON GROUP WISE CYBER FRAUD CASES IN COMMERCIAL BANKS

During the calendar year 2009 total fraud cases reported to the tune of 21966 in Commercial Banks and amount involved there in was Rs.7233.31 lakh. During the calendar year 2009 no. of fraud cases reported in Nationalised Banks were 96 and amount involved was Rs. 98.35 lakh while in State Bank Group only 3 cases were recorded and Rs.7.46 lakh was involved. During the calendar year 2009 in Private Sector Banks no. of fraud cases reported were 16100 and amount involved was Rs.4232.61 lakh while Foreign Banks recorded 5769 fraud cases and amount involved was Rs.2894.89 lakh. During the calendar year 2010, in Commercial Banks no of fraud cases recorded were 15018 and amount involved therein was Rs.4048.94 lakh. During the calendar year 2010, no. of fraud cases reported in Nationalised Banks were 152 and amount involved was Rs.368.65 lakh while in State Bank Group again 3 cases were recorded and Rs1.16 lakh was involved. During the calendar year 2010 in Private Sector Banks no of fraud cases reported were 10130 and amount involved was Rs.2226.25 lakh while Foreign Banks recorded 4733 fraud cases and amount involved was Rs.1452.88 lakh. During the calendar year 2011 in Commercial Banks fraud cases reported were 9588 and amount involved was Rs.3672.19 lakh. During the calendar year 2011 no. of fraud cases reported in Nationalised Banks were 110 and amount involved was Rs.500.29 lakh while in State Bank Group 18 cases were recorded and
Rs 172.19 lakh was involved. During the calendar year 2011 in Private Sector Banks no. of fraud cases reported were 6527 and amount involved was Rs 1670.72 lakh while Foreign Banks recorded 2933 fraud cases and amount involved was Rs 1328.99 lakh. During the calendar year 2012 the reported cases of Cyber Fraud in Commercial Banks were 8322 and amount involved there in was Rs 5266.95 lakh. During the calendar year 2012 no. of fraud cases reported in Nationalised Banks were 118 and amount involved was Rs 689.35 lakh while in State Bank Group 12 cases were recorded and Rs 134.46 lakh was involved. During the calendar year 2012 in Private Sector Banks No of fraud cases reported were 4144 and amount involved was Rs 2506.47 lakh while Foreign Banks recorded 3978 fraud cases and amount involved was Rs 1936.67 lakh.

**B) LEGAL REMEDY AVAILABLE FOR OFFENCES OF CYBER FRAUDS IN BANKING**

Information Technology Act, 2000 and Information Technology Amendment Act 2008 do not define the cyber frauds. However, several provisions of the IT Act, 2000 are relevant for the prevention and control of cyber fraud in India.

**Section 43(b):** When any person without authorization from the owner or any competent person who can give permission accesses, downloads, copies or extracts any data, computer data base or information from any computer, computer network, computer system, computer data or data base or data stored in removable medium i.e. CD, Floppy, DVD and so forth or causes similar damage, he shall be liable to pay maximum Rs. 1 crore compensation.

**Various provisions of the IPC, 1860** are relevant which prohibit and prescribe punishment for fraudulent activities. The IPC has been amended to give effect to the IT Act, 2000, especially provisions relating to cheating and dishonestly inducing delivery of property or valuable security under section 420 IPC, forgery under section 467 IPC, punishment for forgery under section 467 IPC, forgery of valuable security under section 467 IPC, using as genuine a forged document under

444 The Information Technology Act; Section 43 (b)
445 The Indian Penal Code, 1860; Section 420
446 The Indian Penal Code, 1860; Section 467
447 The Indian Penal Code, 1860 Section 467
448 The Indian Penal Code, 1860 Section 467
section 471 IPC1860\textsuperscript{449} etc. The word ‘fraudulently’ has been defined in the IPC as “a person is said to do a thing fraudulently if he does that think with intent to defraud, but not otherwise under section 25 IPC1860\textsuperscript{450}

**ATM frauds and Cyber Law in India**

The Cyber Law of India, as contained in the Information Technology Act, 2000 (IT Act, 2000), is also silent on this aspect. Thus, Internet Banking Frauds and credit card frauds are growing in India. To Prevent ATM frauds requires a coordination and cooperative action among the bank, customers and the law enforcement machinery.

The IT Act, 2000, does not contain any specific provisions regarding the ATM Frauds and the traditional law of Indian Penal Code (IPC), 1860, also cannot be relied solely and independently to tackle this problem. Hence India needs a better law for this purpose. Therefore, Praveen Dalal, the Leading Techno-Legal ICT, Cyber Law, Cyber Security and Cyber Forensics specialist of India, commented as:

"The problem of ATM frauds is global in nature and its ramifications have been felt in India as well. Information and Communication Technology (ICT) is forcing Indian legal system to adapt itself as per its requirements. Presently, there is a lack of legal enablement of ICT systems in India and we need good laws in this regard."\textsuperscript{451}

However, preventing ATM frauds is not the individual problem of banks only but it is a threat to the stakeholders and it requires a coordinated and cooperative action on the part of the bank, customers and the law enforcement machinery.

The Reserve Bank of India published the reports of cyber fraud in every financial year. These reports reflects that there is a tremendous rise of crime incidents within a span of four years since FY2009-10 to FY2012-13 under this category. Therefore it gives the impression that there is no adequate and sufficient legal control of cyber crimes like Phishing against e-banking in India. However the IT Act appears sufficient in all respect but it is not competent enough to tackle the problems of such crimes because there are loopholes in the IT Act 2000 and other legislations and the criminals escape easily by

\textsuperscript{449} The Indian Penal Code, 1860 Section 471  
\textsuperscript{450} The Indian Penal Code, 1860 Section 25  
\textsuperscript{451} Dalal Praveen article *ATM frauds and Cyber Law in India* published on Aug 25, 2008
taking the advantage of these loopholes. On the basis of the above our interpretation is that the existing cyber laws are inadequate and insufficient to control the cyber crimes against e-banking in India as there is a massive growth in cyber crime incidents

C) INCIDENTS OF CYBER FRAUDS

1) India’s First ATM Card Fraud

The Chennai City Police have busted an international gang involved in cyber crime, with the arrest of Deepak Prem Manwani (22), who was caught red-handed while breaking into an ATM in the city in June last, it is reliably learnt. The dimensions of the city cops’ achievement can be gauged from the fact that they have netted a man who is on the wanted list of the formidable FBI of the United States. At the time of his detention, he had with him Rs 7.5 lakh knocked off from two ATMs in T Nagar and Abiramipuram in the city. Prior to that, he had walked away with Rs 50,000 from an ATM in Mumbai. While investigating Manwani’s case, the police stumbled upon a cyber crime involving scores of persons across the globe. Manwani is an MBA drop-out from a Pune college and served as a marketing executive in a Chennai-based firm for some time. Interestingly, his audacious crime career started in an Internet cafe. While browsing the Net one day, he got attracted to a site which offered him assistance in breaking into the ATMs. His contacts, sitting somewhere in Europe, were ready to give him credit card numbers of a few American banks for $5 per card. The site also offered the magnetic codes of those cards, but charged $200 per code. The operators of the site had devised a fascinating idea to get the personal identification number (PIN) of the card users. They floated a new site which resembled that of a reputed telecom company’s. That company has millions of subscribers. The fake site offered the visitors to return $11.75 per head which, the site promoters said, had been collected in excess by mistake from them. Armed with all requisite data to hack the bank ATMs, the gang started its systematic looting. Apparently, Manwani and many others of his ilk entered into a deal with the

452 http://www.indiaforensic.com/atmfraud.htm
gang behind the site and could purchase any amount of data, of course on certain terms, or simply enter into a deal on a booty-sharing basis. Meanwhile, Manwani also managed to generate 30 plastic cards that contained necessary data to enable him to break into ATMs.

On receipt of large-scale complaints from the billed credit card users and banks in the United States, the FBI started an investigation into the affair and also alerted the CBI in New Delhi that the international gang had developed some links in India too. Manwani has since been enlarged on bail after interrogation by the CBI. But the city police believe that this is the beginning of the end of a major cyber crime

2) Three in one fraudster Amit Tiwari trapped for Credit Card Frauds

Amit Tiwari 21-year-old engineering student from Pune had opened bank accounts on different fictitious names. He tried to defraud a Mumbai-based credit card processing company, CC Avenue, by Rs 900,000.

CC Avenue verifies and validates credit cards of buyers for over a thousand e-commerce Web sites. It conducts checks like IP mapping, zip code mapping and reverse lookup of telephone numbers. Amit Tiwari found a way to bypass them. In May 2002, Col Vikram Tiwari signed up for CC Avenue's services. In November, he requested the company to deal with his son, Amit, who offered Web designing services on www.mafiaz.com. CC Avenue's security team confirmed his credentials through bank signature verification, driving license and his HDFC Bank debit card. Everything was genuine. Amit processed several transactions, worth Rs 311,508, via CC Avenue from November 2002 to February 2003. Then the transactions stopped.

In April 2003, CC Avenue began receiving charge-backs from the credit card holders, who denied using mafiaz.com's Web designing service. Amit had assumed the identities of these 'customers', and purchased mafiaz.com's services with credit card details that he found on the Net. He was both the buyer and the seller. Calls to Amit's house in Lucknow went unanswered. Legal notices came back unclaimed. Amit had disappeared without a trace.

In June 2003, Sachin Deshpande and Jeevan Palani signed separate agreements with CC Avenue to provide Web designing services through their sites www.infocreek.org

---

453 Source://www.tribuneindia.com/2005/20050825
and www.ewebsitestarter.com. The company’s risk-management team found that both these sites had ripped off content and even the client list from foreign sites with similar names. The modus operandi was similar to Amit’s case.

Vishwas Patel, the CEO of CC Avenue, spoke to Sachin over the phone and found that he sounded just like Amit - "young and immature". They decided to hold back payment. Then, a person called Shoaiab Sharif sought the services of CC Avenue. Vishwas and his team again spotted a similar pattern. They held back payment on various pretexts. "He sounded desperate," says Vishwas. So they decided to trap him. CC Avenue’s accounts manager asked Shoaiab to come to Mumbai to collect a cheque of Rs 40,000. On August 21, a young man walked into Vishwas’s office. He introduced himself as Shoaiab Sharif. Vishwas immediately recognized him as Amit. (He had seen Amit’s photograph from his driver's license). Vishwas then called the Mumbai Police, who rushed to his office and picked up the lad. At the Santa Cruz police station, the boy confessed right away.

**Amit Tiwari was arrested by the Mumbai Police on August 21, 2003 and charged for cheating under Section 420.**

3) **Labourer held in net banking fraud case**

The cyber crime cell of the Pune police made its first arrest in the net banking fraud case in which former director of the Indian Institute of Technology (IIT), Kanpur, Sanjay Dhande, was duped of Rs 19 lakh.

The police arrested a labourer, Gajanan Tirlotkar (35), of Lower Parel in Mumbai for allegedly allowing the cheats to transfer some of the siphoned-off money into his bank account. Seeking Tirlotkar’s remand, the police told the court that they needed to recover the ATM card which he had used to withdraw the Rs 1 lakh that had been transferred to his account. The police also told the court that they have got details of eight bank transactions through which Dhande’s money had been transferred. The police are trying to trace these bank account-holders, their cell phone numbers and call details of the last six months.

Dhande, a Padma Shree recipient who is also a member of the national Security Advisory Board, had lodged a complaint with the Chatushrungi police station on September 14, 2013 that his account had been hacked between September 6 and 8. As many as 22 online transactions had been made from Dhande's account. Four of these were cash transfers and 18 shopping transactions. Dhande had said he did not get any alerts from the bank after these transactions were made. The fraud came to light after he got an SMS saying the deposits in his account had dipped below a certain amount. The case was later transferred to the cyber crime cell. Inspector Sanjay Tungar of the cyber crime cell, who is investigating the case, told TOI that the cheats had made two equal transactions of Rs 50,000 to Tirlotkar's bank account in Mumbai. A senior police officer from the cyber crime cell said that it was common for cheats to transfer siphoned-off money into the bank accounts of other people so that they themselves could not be traced by the police. The cheats lure these account holders by promising them a part of the amount.

D) LEGAL CASE RELATED TO OFFENCES OF CYBER FRAUDS IN BANKING
1) The Cyber Law Society of India Vs Mr. Vijay Prakash & Others May 5, 2011 Appeal No 4/4010 & MA No.5/2010 in CYBER APPELLATE TRIBUNAL

Present appeal has been filed with the following prayers

“Adjudicating Authority” under the IT Act 2000 be pleased to
a) Direct CERT-IN to investigate and take appropriate action to stop illegal online lotteries being conducted by the Respondents and others.
b) Direct CERT-IN to block access to the aforesaid illegal online lotteries being conducted by the respondent and others.
c) Direct the Government of India to prosecute and take action to ensure that illegal online lotteries do not operate on the internet in so far as the citizen of India are concerned.
d) Direct the aforesaid respondent to pay compensation as may be deemed just and proper for running/conducting/operating illegal online lotteries to the exchequer that represents the general public used in India.

After notice to the respondent, Shree Sunderlal Advocate appeared for the respondent.
The learned Justice Rajesh Tondon on 05/05/2011 has given the judgment that today the learned counsel for the appellant wants to withdraw the appeal for which learned counsel for the respondent that no objection. In view of the aforesaid the present appeal is permitted to be withdrawn. No orders as to cost.

2) SH. Harish Kumar C. Vakaria (Appellant) Vs M/s India Infoline Ltd (Responded) 
APPEAL NO. 1/2009 in CYBER APPELLATE TRIBUNAL 

Date of decision 26/10/2010 
Justice Rajesh Tandon, Chairperson Heard Mr. Manan S. Thakker, Advocate assisted by Mr. Hardik Gupta, Advocate for the appellant and Mr. Y.H. Motiramani, Advocate for the respondent. By the present appeal, the appellant has prayed for the setting aside of the impugned order-in-original No. SEC/ CBC/ I/ 2009/160 DST dated 20th May, 2009 passed by Sh. Raj Kumar, Adjudicating Officer, Gujarat State whereby dismissing the petition filed by the petitioner, appellant herein, under Section 43 of the Information Technology Act, 2000.

Briefly stated the facts of the present appeal are that on 18th January, 2008 Online Demat Account was opened by India Infoline Ltd. A/C No. 1204470001776230 and POA ID was given as VAHARISH. It is stated that ownership of Online Trader Terminal Software was given i.e. access to Online Trader Terminal Software for the said POA ID (Client ID- VAHARISH). On 22nd February, 2008, an application was made by the appellant for the Initial Public Offer of Rural Electrification Corporation Ltd. (REC Ltd.) in the name of Harishkumar Chandrakant Vakharia (HUF). Cheque Number was 163127, cheque amount was Rs. 94,500/-, Bank name was ICICI Bank, S.G. Road branch and the Bank A/C number was 029501001050 of HUF saving account Appellant has submitted that on 7th March, 2008, Karvy.com displayed allotment of 121 (amount Rs. 12,705/-) shares of REC Ltd. and remaining amount of Rs. 81,795/- came to be credited into the above mentioned bank account. It is further submitted that the said shares were not credited in the appellant’s online Demat Account after they were allotted. A message was alleged to have been displayed that Online Demat Account is closed. A similar letter was also sent by Karvy on 11th March, 2008. According to the appellant, due to unauthorized suspension, the amount of Rs. 94,500/- could not be paid
back to Mrs. Veena Baxi, Creditor as per commitment on 8.3.2008 i.e. the due date for making payment to the said creditor. According to the appellant he was deprived of investment of 121 shares of REC Ltd. which remained blocked from 22.8.2008 to 18.9.2008 (28 days), therefore, the entire conduct of the India infoline Ltd. is fraudulent and the appellant has suffered a loss on account of the same.

The appeal was contested by the respondent by denying the averments contained therein. It was submitted that the respondent has not committed any offence or that there was unauthorized access-suspension-disruption-damage to Online Demat Account or Trading Terminal Software as alleged or otherwise. Heard the counsel for the parties.

Following points arise for consideration in this appeal.

(i) Whether the appeal was within time?
(ii) Whether the appellant has suffered a loss on account of the suspension of demat account?
(iii) Whether necessary parties are represented in order to decide the complaint?
(iv) Whether there was any arbitration clause and the matter was not liable to be adjudicated under Section 43 of the Information Technology Act?

The learned Judge given the point wise decision as under:

Point No.(i):- Point no. 1 is decided in the negative.

Point No.(ii):- Thus, the petitioner has failed to establish the primary requirement for applicability of section 43 of the Information Technology Act that the respondent’s actions were without the permission of the owner of the computer, computer systems or computer network.” The Adjudicating Officer shall give the respondent sufficient opportunity to represent his case on merits. The point is decided accordingly.

Point No.(iii):- The appellant is, therefore, directed to implead CDSL, BSE and NSE as parties before the Adjudicating Officer. The Adjudicating Officer shall give sufficient opportunity to the parties to lead evidence in respect of their claim and defense including the newly added parties. This point is decided accordingly.

Point No.(iv):- In view of aforesaid discussion, this point is decided accordingly with a direction to the Adjudicating Officer to decide regarding the applicability of Section 8 of the Arbitration and Conciliation Act first i.e. on the point No.(iv) referred above and
thereafter to proceed on other points

Relief:- In view of the above, the matter is remanded to the Adjudicating Officer, Gujarat State for deciding afresh in view of observations made above. Parties are directed to appear before the Adjudicating Officer, Gujarat State on 5th July, 2010. This appeal is disposed of accordingly and the parties have to bear their own costs in the appeal.

Other cases decided by CAT (Cyber Appellate Tribunal)


Hon’ble Mr. Justice Rajesh Tandon Chairperson decided the appeal on 28/05/2010 and decided that the appeal lacks merit and is dismissed at the admission stage.

Pending cases of frauds under various section of the IT Act

1) Case No.99/2008 Purchase of airline tickets Frauds
This case was registered under Section 66 of the IT Act and relates to purchase of airline tickets in four transactions of Rs.7200/- each and is still under investigation.

2) Case No. Cr.No.131/10 Complaint under hacking, theft and cheating
This case was registered under Section 379 IPC & 66(c), 66(d), 67(a) of the IT Act is a complaint of hacking, theft and cheating. In this case the accused was arrested on 16.4.2010 and the case is still under investigation.

3) Case No. Cr.No.126/10 Complaint of Ms. Sandhya Pandurang Naik
This case was registered under Section 66(C) of the IT Act is a complaint filed on 6.5.2010 by Ms. Sandhya Pandurang Naik stating that some unknown accused person created false E-mail ID of the complainant lady as Sandhya Naik @Gmau.com and thereby committed theft of e-mail. The case is under investigation.

4) Case no Cr.No.74/2009 relates to false e-mail of winning of COCO COLA Contest.
The case was registered under the Section 420 IPC read with Section 66 of the IT Act, 2000 where a false e-mail was sent directing the complainant to deposit an amount
of Rs.1,69,420/- as he has won the COCO COLA contest of one lakh Pounds. On the investigation the culprit was arrested at Imphal East Manipal.

5) Fraud case of Elite Creative account with ICICI Bank New Delhi.
This case was under Section 420 IPC is still under investigation read with Section 66 of IT Act,2000 was filed for depositing a sum of Rs.35000/- towards custom charges to Elite Creative with PAN No.AMGPA2286A, ICICI Bank branch New Delhi. This case is still under investigation

6) Case No.72/2009 Fraud case of purchase travelling tickets from HDFC Bank
This case was registered under Section 66 of the IT Act, 2000. In this complaint the complainant complained that some unknown accused person gained access without permission to the computer system of HDFC Bank and purchased tickets for travel worth Rs.30,000/-. This case is still under investigation.

3.4.4. (II) PROBLEMS OF DATA THEFT IN E-BANKING IN INDIA
Due to the swift expansion of Information Technology in the World in general and banking in particular created new problems before the law. These problems are not limited to any statute alone but occur in all the existing statute likes for example, Contract Law, Banking Law, Criminal Law, Evidence Law and Intellectual Property Law. Data Theft is the brain child of Information Technology. Now a day, banking industry is facing the problem of data Theft. When any information in the form of data is illegally steal from the computer or computer network from a business and corporate houses, organisations like banks and individual persons without their knowledge or consent.

A) DEFINITION OF DATA
The Information Technology Act, 2000, Sec. 2(1)(o) ‘data’ means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.
B) PROBLEM OF DATA THEFT IN THE BANKING INDUSTRY

The most important problem regarding Data Theft in banking is its easily access to the computers and computer network from anytime and anywhere from the world and bears the international nature. The example can be cited as banking systems can be accessed in one country other than India and the data manipulated in another country. The host country like India or Bangladesh has to face the consequences. Major problem for prevention of “Data Theft” is the law of the different countries, their problem of jurisdictions, regional laws and rules came into the way for controlling the crime of data theft. Another problem of law is the evidence collection. In the given situation it is the Herculean task to collect the evidence from different countries. There is no harmony of law between the various countries. There is no specific international treaty for extradition of offenders of data theft. Moreover the provisions of Information Technology Act are inadequate and insufficient to control the cyber crime like Data Theft. Therefore even though the criminal is nabbed under the charge of cyber crimes like Data Theft he easily rescued by taking the benefits of various loopholes in Information Technology Act. Offences covered under the Data Theft in banking are 1) Trojan horse & Bugbear, 2) Website Compromise Malware Propagation, 3) Phishing & Hacking, 4) Soofing, 5) Network scanning

C) LEGAL REMEDY AVAILABLE FOR OFFENCES OF DATA THEFT AGAINST E-BANKING IN INDIA

Though the problem of data theft is most significant cybercrime committed globally, the law makers in India has not paid more attentions towards the problem of data theft. India has enacted Information Technology Act, 2000 to address the ever growing threat of cyber crimes which also includes data theft but there is no specific legislation in India to tackle this problem The ground reality of IT Act, 2000 is that it is not well outfitted to tackle the cyber crimes like Data Theft in banking, other organization and individuals. The IT Act 2000 not directly deals with the problem of Data Theft but deals with the problem up to some extent. Let us discuss the legal remedy available for Data Theft as under
EXISTING LEGAL FRAMEWORK FOR DATA PROTECTION IN INDIA

a) Legal protection under Information Technology Act, 2000

(1) Section 43 provides protection against destruction and unauthorized access of the computer system by imposing heavy penalty up to one crore. The unauthorized downloading, extraction and copying of data are also covered under this section. Clause ‘C’ of this section imposes penalty for unauthorized introduction of computer viruses of contaminants. Clause ‘G’ provides penalties for assisting the unauthorized access

(2) Section 65 provides for computer source code. If anyone knowingly or intentionally conceals, destroys, alters or causes another to do as such shall have to suffer imprisonment of up to 3 years or fine up to 2 lakh rupees. Thus protection has been provided against tampering of computer source documents.

(3) Section 66 provides Protection against hacking has been provided under this section. As per this section, hacking is defined as any act with an intention to cause wrongful loss or damage to any person or with the knowledge that wrongful loss or damage will be caused to any person and information residing in a computer resource must be either destroyed, deleted, altered or its value and utility get diminished. This section imposes the penalty of imprisonment of up to three years or fine up to two lakh rupees or both on the hacker.

(4) Section 70 provides protection to the data stored in the declared protected systems in gazette, Protected systems includes those computers, computer system or computer network which were declared by the appropriate government, by issuing gazette information in the official gazette and declared it as a protected system. Any access or attempt to secure access of such protected system will be liable for punishment of imprisonment which may extend to ten years and shall also be liable to fine

(5) Section 72 provides any person upon whom powers have been conferred under IT Act and allied rules to secure access to any electronic record, book, register, correspondence, information document of other material discloses it to any other person, shall be punished with imprisonment which may extend to two years or with fine which may extend to one lakh rupees or both.
b) Legal protection under IT Amendment Act, 2008
IT Amendment Act, 2008 requires all foreign corporations with offshore Indian service partners to maintain “reasonable security practices and procedures” when handling “sensitive personal data”
(1) **Section 43A** provides a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected. This section does not define the phrase reasonable security practices, and procedures. The phrase is determined as defined between the parties by mutual agreement or as specified in any law for the time being in force or to be specified by the Central Government in consultation with such professional bodies or associations as it may deem fit.
(2) **Section 72A** provides disclosure of information in breach of lawful contract any person including an intermediary who; while providing services under the terms of lawful contract; has secured access to any material containing personal information about another person; with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain; discloses; without the consent of the person concerned, or in breach of a lawful contract; such material to any other person; and shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

c) Legal protection under Indian Penal Code, 1860
(1) **Section 378 of I.P.C., 1860** provides whoever, intending to take dishonestly any movable property out of the possession of any person without that person’s consent, moves that property in order to such taking, is said to commit theft.
(2) **Section 22 of I.P.C., 1860** defines “movable property” are intended to include corporeal property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth.”
From the above it reveals that Section 378 I.P.C. only refers to “Movable Property” while Data by is not covered under the definition of "Theft". It is pertinent to note here that Data itself is intangible. On the other hand if Data is stored in gadget/device like CD, Removable Disc etc. and if such gadget/device is stolen, it would be covered under the definition of ‘Theft’, since gadget/device is a movable property. However, if Data is transmitted through electronic means, it would be termed as in the intangible form and therefore it would not be constituted as theft under the IPC.

**Data Protection with respect to Banking Sector**

Data Protection is an essential characteristic in the banking sector due to the nature and sensitivity of the data. The amendments made to the IT Act, 2000 by the Amendment Act, 2008 seems to be mid way between the two as far as norms guiding the protection of personal data exported to India are concerned. Section 43A of IT Act deals with the aspect of compensation for failure to protect data. Whether Section 43A read with Section 72 and 72A of the IT Act, 2000 present address the issue of data protection adequately or they need to be duly supplemented by long-term provisions which can help facilitate effective and efficient protection and preservation of data would depend on the prescriptions of the Central Government. The provisions of the Information Technology Amendment Act 2008 are vague on the data protection in banking sector. However the IT Act appears sufficient in all respect but it is not competent enough to tackle the problems of such crimes because there are loopholes in the IT Act 2000 and other legislations and the criminals escape easily by taking the advantage of these loopholes. On the basis of the above our interpretation is that the existing cyber laws are inadequate and insufficient to control the cyber crimes against e-banking in India as there is a massive growth in cyber crime incidents.

**D) LEGAL CASE RELATED TO OFFENCES OF DATA THEFT IN BANKING**


“Data”, in its intangible form, can at best be put at par with electricity. The question whether electricity could be stolen, arose before the Hon’ble Supreme Court in the case.

---

455 Report & Recommendations of the working group of information security, electronic banking technology, risk management and cyber fraud published by RBI on January 2011
“Avtar Singh vs. State of Punjab” (AIR 1965 SC 666). Answering the question, the Supreme Court held that electricity is not a movable property, hence, is not covered under the definition of ‘Theft’ under Section 378 IPC. However, since Section 39 of the Electricity Act extended Section 378 IPC to apply to electricity, so it so became specifically covered within the meaning of “Theft”. It is therefore imperative that a provision like in the Electricity Act be inserted in the IT Act, 2000 to extend the application of section 378 IPC to data theft specifically.

2) Umashankar Sivasubramaniam Vs ICICI bank (Petition No. 2462/2008 dated 18.04.2010)
Umashankar Sivasubramaniam case decided against ICICI bank (phishing fraud) The adjudicating Officer held that The Respondent bank has failed to put in place a foolproof Internet Banking system with adequate levels of authentication and validation which would have prevented unauthorized access found guilty of the offences made out Award Rs. 12.85 lakh compensation under section 85 r/w section 43 of the Act (The case is already discussed in the foregoing paragraphs of problem of mounting phishing cases)

3) Nasscom Vs Ajay Sood and Others (23March 2005) in Delhi High Court
Delhi High Court declared phishing on the internet to be an illegal act, entailing injunction and recovery of damages. Personal data was illegally collected by misrepresenting the identity of legitimate party. Delhi High Court held that “misrepresentation made in the course of trade leading to confusion as to the source and origin of the e-mail causing immense harm not only to consumer but even to the person whose name, identity or password is misused. Delhi High Court awarded Rs.1.6 million compensation against the defendants. (The case is already discussed in the foregoing paragraphs of problem of mounting phishing cases)

456 119(2005)DLT596, 2005(30)PTC437(Del)
This appeal was filed against the order dated 27.07.2009 of the District Consumer Disputes Redressal Forum, Raigarh directing the appellant bank to pay 49,912.36/-, which was allegedly not withdrawn by him from his account and also 5,000/- as compensation for mental agony and 3,000/- as litigation cost to the respondent/complainant on account of deficiency in service, regarding maintenance of his bank account. The complaint was filed alleging deficiency of service on the part of the appellant bank as 49,912.36/- was withdrawn from his bank account, without his knowledge, using internet banking. The State Commission vide its order dated 26.03.2010 allowed the appeal. The Commission observed that the respondent was negligent in giving information regarding password to a third person and hence deficiency of service could not be attributed on the part of the appellant bank, who had taken all precaution to give every instruction to the customer and also authorized him to change his password as and when desired.

5) Rishi Gupta v. ICICI Bank Ltd. - Before the Consumer disputes Redressal Forum, Bangalore-(CC No. 514 of 2010)
The complaint sought an order directing opposite party bank to refund 2,30,000/- along with interest @ 24% per annum which was lost by the complainant on account of alleged negligence of the opposite party and for an order directing the bank to pay 1,00,000/- as damages for negligence of service. The complainant alleges that an amount of 3,00,000/- was transferred from the account of the complainant, fraudulently, through 15 transactions of 20,000/- each. The District Forum vide order dated 21.06.2010 dismissed the complaint. The Hon'ble member in the order dated 21.06.2010 observed that in providing confidential details of his online banking such as corporate ID, password etc, to a third party in response to an email purported to be issued by the opposite party bank, without verifying with the opposite party bank, the complainant had acted negligently and he cannot put the blame on the bank.
3.4.5. (III) PROBLEM OF CYBER TERRORISM AGAINST E-BANKING IN INDIA

A) Meaning and Definition of Cyber Terrorism

Meaning :- Information technology (IT) has created an opportunity to the public by rendering an enormous data of information regarding each and everything available on net. This opportunity has also added a new challenge of terrorism. Recent reports suggest that the terrorist is also getting equipped to utilize cyber space to carryout terrorist attacks. Terrorism related to cyber is popularly known as 'cyber terrorism'.

In the last few of decades India has engraved a position for itself in IT. Almost Indian banking industry and financial institutions have adopted Information Technology for providing the e-banking services to customers. In addition to regular computer crimes such as fraud and identity theft, attacks against critical information infrastructures could become a goal for terrorists. The growing reliance on information technology makes critical infrastructure more vulnerable to attacks. This is especially the case with regard to attacks against interconnected systems that are linked by computer and communication networks. In those cases, the disruption caused by a network-based attack goes beyond the failure of a single system. Even short interruptions to services could cause huge financial damage to e-commerce businesses – not only for civil services but also for military infrastructure and services. Investigating or even preventing such attacks presents unique challenges. Unlike physical attacks, the offenders do not need to be present at the place where the effect of the attack occurs. And while carrying out the attack the offenders can use means of anonymous communication and encryption technology to conceal their identity.

Definition:- 'Cyber terrorism is the convergence of terrorism and cyber space. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Terrorist may

---

457 Raghav S. S.Colonel Article Cyber Security in India’s counter terrorism security
Source:http://ids.nic.in/art_by_offids
direct an attack only to disrupt key services, if they create panic by attacking critical systems/infrastructure there is no need for it to lead to violence. In fact such attacks can be more dangerous\textsuperscript{458}

**METHODS OF CYBER TERRORISM ATTACKS**\textsuperscript{459}

The methods on the computer infrastructure can be classified into three different categories.

**(a) Physical Attack.** The computer infrastructure is damaged by using conventional methods like bombs, fire etc.

**(b) Syntactic Attack.** The computer infrastructure is damaged by modifying the logic of the system in order to introduce delay or make the system unpredictable. Computer viruses and Trojans are used in this type of attack.

**(c) Semantic Attack.** This is more treacherous as it exploits the confidence of the user in the system. During the attack the information keyed in the system during entering and exiting

**TOOLS OF CYBER TERRORISM AGAINST E-BANKING IN INDIA**

Following are the tools of cyber terrorism against banking

**(a) Hacking:** The most popular method used by a terrorist. It is a generic term used for any kind of unauthorized access to a computer or a network of computers. Some ingredient technologies like packet sniffing tempest attack, password cracking and buffer outflow facilitates hacking.

**(b) Trojans:** Programmes which pretend to do one thing while actually they are meant for doing something different, like the wooden Trojan Horse of the 12\textsuperscript{th} Century BC.

**(c) Computer Viruses:** It is a computer programme, which infects other computer, programmes by modifying them. They spread very fast.

**(d) Computer Worms:** The term ‘worm’ in relation to computers is a self contained programme or a set of programmes that is able to spread functional copies of itself or its segments to other computer systems usually via network connections.

\textsuperscript{458} Raghav S. S.Colonel Article Cyber Security in India’s counter terrorism security

\textsuperscript{459} ibid
(e) E-Mail Related Crime:- Usually worms and viruses have to attach themselves to a host programme to be injected. Certain emails are used as host by viruses and worms. E-mails are also used for spreading disinformation, threats and defamatory stuff.

(f) Denial of Service:- These attacks are aimed at denying authorized persons access to a computer or computer network.

(g) Money Laundering:- Under the Prevention of Money Laundering Act (PMLA), 2002, a suspicious transaction includes a transaction that gives rise to a reasonable ground of suspicion that it might be involved in financing of the activities relating to terrorism. The law defines such transactions as those involving funds suspected to be linked or related to or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism. But government does not conclude that all suspicious transactions would relate to terror acts since it lists several other parameters broadly under money laundering activities.

(All the methods describe above are discussed in detail in chapter 2.4 “Types of cyber crimes against e-banking”.

Terrorist financing

The sources of finance of terrorist organizations depend on the third parties by way of donation or by accepting the money in some other form. There are several ways in which Internet services can be used for terrorist financing. Terrorist organizations mostly use electronic payment systems to enable online donations. They also use websites to publish information how to donate, e.g. which bank account should be used for transactions. An example of such an approach is the organization “Hizb al-Tahrir”, which published bank-account information for potential donors. Another approach is the implementation of online credit-card donations. The Irish Republican Army (IRA) was one of the first terrorist organizations that collected donations via credit card. Both approaches carry the risk that the published information will be discovered and used to trace back financial transactions. Another (Internet-related) approach is the operation of fake web shops. It is relatively simple to set up an online shop on the Internet. One of the biggest advantages of the network is the fact that businesses can be operated worldwide.

460 en.wikipedia.org/wiki/Terrorism_financing
B) Facts and Figures of Terrorist Attacks

a) Report of Finance Ministry\(^{461}\): A finance ministry internal report found out that banking companies reported a maximum of 11,840 suspicious transactions between 2006 and 2010. Financial institutions and intermediaries followed with 2,872 and 2,497 suspicious transactions reported respectively during 2006-10.

The report illustrates growing fear of penetration of terror outfits in the banking and financial system of the country. The finance ministry's Financial Intelligence Unit (FIU) has been entrusted with the task to tabulate all Suspicious Transaction Report (STR). FIU is an independent body reporting directly to the Economic Intelligence Council (EIC) headed by the Finance Minister.

b) Financial Intelligence Unit (FIU)\(^{462}\): As per the FIU report over 17,000 suspicious transactions were recorded in all during 2006-2010. The STRs recorded during 2006-07 stood at 817, growing to 1,916 in 2007-08, 4409 in 2008-09 and 10,067 in 2009-10.

c) Suspicious Transaction Report (STR) amongst Commercial Banks in India\(^{463}\): In the banking sector that leads the list of suspicious transactions maximum 5479 STRs were reported by private banks in the country. Public sector banks, foreign banks, insurance companies and mutual funds too reported such transactions with 3878, 2403, 2063 and 1892 STRs recorded by them respectively during 2009-10.

d) Suspicious Transaction Report (STR) amongst Indian States\(^{464}\): Among states, Maharashtra dominated with maximum 29% share in STRs reported in all sectors. Delhi and West Bengal also followed with 12.1 and 7.3% share respectively. Other significant states in terms of share in STRs were Gujarat and Uttar Pradesh at 6%, Tamil Nadu 5.7%, Punjab 5.1%, Karnataka 4.7% and Andhra Pradesh 4.4%. Bihar and Chattisgarh conceded least 1.1% of suspicious transactions between 2006 and 2010. Even though some states like Maharashtra, Delhi and West Bengal still occupy high ranking positions in terms of the number of STRs, there are other emerging states like UP, Punjab, Andhra Pradesh, Haryana and Kerala where the share is on the increase.

---

\(^{461}\) Report of Finance Ministry on STR(Suspicious Transaction Report)
\(^{462}\) Suspicious Transaction Report (STR) published by Financial Intelligence Unit (FIU)
\(^{463}\) Ibid
\(^{464}\) Ibid
C) LEGAL REMEDY AVAILABLE FOR CYBER TERRORISM

A) PROTECTION UNDER I.T.ACT, 2000:

The threat created by the malware for cyber terrorism can be successfully controlled only if provisions of the I.P.C with the strict provisions of the Information Technology Act, 2000 jointly implemented. Courts can use their discretion by combining provisions of various statutes to do the complete justice so long the provisions can operate in the presence of each other. Accordingly, the Indian Penal Code, 1860 and the provisions of ITAct can be add-on with the provisions of I.P.C to control the cyber terrorism.

The protection of ITAct can be claimed for:

(a) Violations of Privacy: Right to privacy is a part of the right to life and personal liberty enshrined under Article 21 of the Constitution of India. The various provisions of the ITAct2000 pertinently protect the online privacy rights of the netizens. The legal remedy available against the culprit using the malware. Section 1 (2) read with Section 75 of the ITAct2000 provides for an extra-territorial application of the provisions of the Act. Thus, if a person (including a foreign national) contravenes the privacy of an individual by means of computer, computer system or computer network located in India, he would be liable under the provisions of the ITAct2000.

(b) Prevention of information and data theft: Provisions of IT Act2000 dealing with the data theft under section 43, section 65, Section 66, Section 70 and Section72 can be successfully invoked. Likewise Provisions of ITAA2008 under section 43A and section 72A jointly supplemented with section 22 of I.P.C.,1860 and 378 of I.P.C.,1860 can be invoked

(c) Prevention of distributed denial of services attack:
A malware may also use the method of distributed denial of services (DDOS) to overburden the electronic bases of individuals. Thus, distribute denial of services by use of malware will be tackled by invoking the provisions of sections 43,section 65 and section 66 of ITAct2000 collectively.

(d) Prevention of network damage and destruction:
In India there is no law, which is specifically dealing with prevention of malware through aggressive defense. Thus, the analogous provisions have to be applied in a purposive
manner. The protection against malware attacks can be claimed under the following categories:

(1) **Protection available under the Constitution of India,**

(a) Article 19(1) (g), (b) Article 21, (c) Article 300A, and (d) Articles 301 to 305.

(2) **Protection available under other statutes.**

(A) **Protection under I.P.C:** (i) Section 22, 23,29, 29A read with Section 2(1) (t) of the IT Act, 2000, Section 32, 33 40,43, 44,96,97,99,268,378 and Section 425 Legal remedy is available under Information Technology (Amendment) Act, 2008, Section 43(c) & 43(e) read with Section 66 and under Section 268 of Indian Penal Code, 1860. Section 65 & 66 are dealt with the offences related with Website Compromise & Malware propagation. The offences are cognizable offences with bailable and compoundable with a permission of the court before which the prosecution of such offence is pending. Section 43 addresses the civil offence of theft of data. Concealing, destroying, and altering any computer source code when the same is required to be kept or maintained by law is an offence punishable with three years imprisonment or two lakh rupees or with both Criminalities in the offence of data theft is being separately dealt with later under Sections 65 and 66.

**3.4.6. (IV) JURISDICTIONAL PROBLEM AGAINST E-BANKING IN INDIA**

During the modern era of information technology, internet plays a pivotal role and became the essential part of the routine life. Due to the advent of Internet, cyber space has to perform the important role in the business transactions. Cyber crime does not know by any geographical boundries and crime committed by the miscreants beyond the boundaries of state makes the state helpless to take any stringent action related to jurisdiction against such miscreants.

Cyberspace does not know any boundaries. The United States Supreme Court's first opinion about the Internet contains language that makes one hopeful that U.S. courts will accept the legal metaphor of cyberspace as a place outside national boundaries. Taken together, these tools constitute a unique medium -- known to its users as
'cyberspace'-- located in no particular geographical location but available to anyone, anywhere in the world, with access to the internet 465 Therefore Cyberspace is a “borderless” world and refuses to accord to the geographical boundaries while the private international law has always concurrence with the geographical boundaries of the state. Therefore there should be different angle to solve the problem as cyber space is entirely different from the real world466.

Definition of the Jurisdiction
“Jurisdiction is defined as the “power of the court to decide a matter in controversy and presupposes the existence of a duly constituted court with control over the subject matter and the parties 467.” As per this definition the power conferred to the court to hear and decide the case on merits. The court's decision holds no water without jurisdiction. The judgment of the court has no effect and importance without jurisdiction.

Basis of the Court’s Jurisdiction
The term “jurisdiction” is used to describe various different legal issues. Based upon principles of public international law “jurisdiction” describes the authority of a sovereign state to regulate certain conduct. It is therefore one aspect of national sovereignty. However, in the context of cybercrime investigation “jurisdiction” refers to the authority of a state to enforce its domestic law. In general, law enforcement will only be able to carry out an investigation if the country has jurisdiction.468

Jurisdiction in the Cyber Space
Cybercrime is a typical transnational crime that involves different jurisdictions. It is not unusual that several countries are affected. The offender might have acted from country A, used an Internet service in country B and the victim is based in country C. This is a challenge with regard to the application of criminal law and leads to questions about which of the countries jurisdiction, which country should take forward the investigation has and how to resolve disputes. While this case looks already challenging it is

465 Darrel Menthe in Article Jurisdiction In Cyberspace :A Theory of International Spaces
466 Sachdeva A.M. in Article International Jurisdiction of cyber space, A comparative perspective
necessary to take into consideration that if the offence, for example, involves cloud computing services even more jurisdictions may be triggered.469

Online transaction has raised a new question of jurisdiction in cyber space. This is an attempt to resolve the question of jurisdiction in the cyber space. Due to advancement of information technology and its adoption in banking sector promotes the business at national as well as international level. Due to the dawn of internet and computer technology, communication become easiest in application and cheapest in cost. Internet crossed the geographical boundaries of the nations and reached every nook and corner of the world. This aspect of internet has ignored crossed the international boundaries. As and when any intercontinental transaction took place with the help of internet there are very reasonable chances of dispute to be taken place amongst the parties to the transaction. This dispute may give birth to the conflict of law. The reason behind this is the different statuette in the different countries and therefore the applicable law changed is as per the change of the country. There may be the conflicts and difference of opinion between the countries due to difference in their culture, dissimilarity in their demography, disparity in their systems and their moral values. The information on the WEB(WWW)can be accessed by anybody from anywhere in the world. This aspect can originate many legal issues. The most important such issue is the issue of Jurisdiction over the cyber crime. The internet banking is also facing the problem of jurisdiction in the cyber space.470

**TYPES OF JURISDICTION**

Following are three types of jurisdiction generally recognized in international law.

(1) The jurisdiction to prescribe;

(2) The jurisdiction to enforce; and

(3) The jurisdiction to adjudicate

The jurisdiction to prescribe is the right of a state to make its law applicable to the activities, relations, the status of persons, or the interests of persons in things. The jurisdiction to enforce is the right of the state to enforce the statute and jurisdiction to adjudicate are the geographical boundaries of the state to adjudicate.


470 Manikyam SITAM K Dr. Cyber Crimes Law & policy perspectives, hind law house Pune 2009 edition p184
THEORIES OF JURISDICTION UNDER INTERNATIONAL LAW

Under international law, there are six generally accepted bases of jurisdiction or theories under which a state may claim to have jurisdiction to prescribe a rule of law over an activity. In the usual order of preference, they are as under:

1. Subjective Territoriality.
2. Objective Territoriality,
3. Nationality.
4. Protective Principle,
5. Passive Nationality and
6. Universality

As a general rule of international law, even where one of the bases of jurisdiction is present, the exercise of jurisdiction must be reasonable.

1) Subjective territoriality: The forum state has the jurisdiction to prescribe a rule for the activity which takes place within the territory of the forum state. The most of the criminal legislation in the world is belongs to this category.

2) Objective territoriality: When the action takes place outside the territory of the forum state then this type of territoriality is invoked but the primary effect of that activity is within the forum state. The classic case is that of a rifleman in Canada shooting an American across Niagara Falls in New York. The shooting takes place in Canada; the murder -- the effect -- occurs in the United States. The United States would have the jurisdiction to prescribe under this principle.

3) Nationality:-Nationality is the basis for jurisdiction where the forum state declares the right to prescribe a law for an action based on the nationality of the person who performed the action. Under the law of the Netherlands, for example, a Dutch national "is liable to prosecution in Holland for an offence committed abroad, which is punishable under Netherlands law and which is also punishable under the law of the country where the offence was committed." Many other civil law countries have similar laws.

4) The Protective principle: - The protective principle expresses the desire of a sovereign to punish actions committed in other places solely because it feels threatened.

471 Darrel Menthe in Article Jurisdiction In Cyberspace :A Theory of International Spaces
by those actions. This principle is invoked where the "victim" would be the government or sovereign itself. For example, in *United States v. Rodriguez* the defendants were charged with making false statements in immigration applications while they were outside the United States. This principle is disfavored for the obvious reason that it can easily offend the sovereignty of another nation.

5) **Passive nationality:** - It is a theory of jurisdiction based on the nationality of the victim. Passive and "active" nationality are often invoked together to establish jurisdiction because a state has more interest in prosecuting an offense when both the offender and the victim are nationals of that state. Passive nationality is rarely used for two reasons. First, it is offensive for a nation to insist that foreign laws are not sufficient to protect its citizens abroad. Second, the victim is not being prosecuted. A state needs to seize the actor in order to undertake a criminal prosecution.

6) **Universality:** - The final basis of jurisdiction is universal jurisdiction, sometimes referred to as "universal interest" jurisdiction. Historically, universal interest jurisdiction was the right of any sovereign to capture and punish the bandit. This form of jurisdiction has been expanded during the past century and a half to include more of *jus cogens*: slavery, genocide, and hijacking (air piracy). Although universal jurisdiction may seem naturally extendable in the future to Internet piracy, such as computer hacking and viruses, such an extension is unlikely given the traditional tortoise-like development of universal jurisdiction. It is pertinent to note here that universal jurisdiction traditionally covers only very serious crimes. Therefore all nations have due process type problems with convictions under this principle.

**Flag principle**

The flag principle is closely related to the principle of territoriality but extends the application of domestic laws to aircrafts and ships. Taking into account the availability of Internet access solutions for maritime and air transportation raises questions related to the application of criminal law in cases where either the offender, victim or affected computer systems is not located in the territory but outside the territorial borders of country on board of a ship or aircraft.
**Doctrine of international jurisdiction**

Based on the international law, each state should respect to the sovereignty of other states and not to interfere by the other states in the sovereignty of each state. Every state should have to respect the sovereign equality and peaceful co-existence where territoriality is the inevitable consequence of each state. Personal and perspective Jurisdictional principle were originally derived from the assumption that every states have absoluteness of boundaries and sovereign power in them. Considering the territorial nature of sovereignty as a universal rule jurisdiction extends to everybody and everything within the territory of sovereignty and to his nationals wherever they maybe.

**Cyber Space and Traditional Jurisdictional Concept**

The internet has its own limitations. It has its own specific features. Internet is the medium to connect the people from every nook and corner of the world. The configuration of the Net is such that there is no real means of avoiding contact with a specific jurisdiction.

**Traditional requirements cover two areas:**

1) The place of resident of the defendant
2) The place where cause action arises.

But in the cyber space, the principle of traditional jurisdiction does not applied. The internet does not bound by any physical geographical limits therefore traditional principles of jurisdiction do not apply on it. For example Mr. A from India downloads a document through net and makes payments through credit card. While downloading the document he found that it was incomplete. He wants to sue the owner of the site. But the owner is residing in America and the site is located on the server at New Zeeland. There is confusion while deciding the residential status of the defendant. In such circumstances it is worth important to examine the case laws relating to Internet jurisdiction. While discussing the myriad of case laws on the internet jurisdiction we have to segregate the case laws into different categories like “Advertise on the Net”, Defamation etc, and to observe how the Judiciary in US struggle to keep fit the law as

---

472 Sachdeva A.M. in Article International Jurisdiction of cyber space, A comparative perspective
per the changing need of the society and as per the of the adoption of the new technology.\textsuperscript{473}

\textbf{THE POSITION IN INDIA}

\textbf{Personal jurisdiction}

No rule of procedure of foreign law is recognised. It was held in \textit{Ramanathan Chettier v Soma Sunderam Chettier}\textsuperscript{474} that India accepts the well-established principle of private international law that the law of the forum in which the legal proceedings are instituted governs all matters of procedure. In India, the law of personal jurisdiction is governed by the Code of Civil Procedure 1908 (the Code). The Code does not lay any separate set of rules for jurisdiction in case of international private disputes\textsuperscript{475}. It incorporates specific provisions for meeting the requirements of serving the procedure beyond territorial limits. In the matter of jurisdiction what is treated differently is the question of subject-matter competence and not of territorial competence, i.e. the question of territorial jurisdiction arises in the same way in an international private dispute as in a domestic dispute.

The Code provides general provisions regarding jurisdiction on the basis of pecuniary limit, subject matter and territory. Sections 16 to 20 of the Code regulate the issue of territorial jurisdiction for institution of suits.

\textbf{Rules as to the nature of suit}\textsuperscript{476}

Based on the subject-matter suits are divided into three classes:

\begin{itemize}
  \item[(1)] suits in respect of immovable property;
  \item[(2)] suits for torts to persons or movable property; and
  \item[(3)] suits of any other kind.
\end{itemize}

Suits of immovable property must be filed within the local limits of whose jurisdiction the property situated\textsuperscript{477}. The Code therefore incorporates the principle of \textit{lex situs} and therefore the property in this section may refer to only property “situated in India”.

\textsuperscript{473} Manikyam SITA . K. Dr Cyber Crimes Law & policy perspectives, hind law house Pune 2009 edition p197
\textsuperscript{474} AIR 1964 Madras see also Nallatamlei v Ponuswami BR[1879]2 Madras406
\textsuperscript{475} See ss.9 and 15 of the Code of Civil Procedure 1908.
\textsuperscript{476} Sachdeva A.M. in Article International Jurisdiction of cyber space, A comparative perspective
\textsuperscript{477} The Code ss.16 and 17.
Suits for wrongs to persons and movable property may be instituted in the courts within whose local limits the wrong is done or the defendant resides or carries on business or personally works of gain\(^\text{478}\). Suits of any other kind are dealt with under s.20 of the Code which is the “default rule” providing for all others cases not covered by any of the foregoing rules. Under s.20, a court can exercise jurisdiction in actions involving persons where:

(a) the defendant, or each of the defendants where there are more than one, at the time of the commencement of the suit, actually and voluntarily resides, or carries on business, or personally works for work; or

(b) any of the defendants, where there are more than one, at the time of commencement of the suit actually and voluntarily resides, or carries on business, or personally works for gain, provided that in such case with the leave of the court has been obtained or the defendants who do not reside or carry on business, or personally work for gain, as aforesaid, acquiesce in such institution; or

(c) The cause of section wholly or partly arises.

**Jurisdiction of Civil Courts in India**

In India, civil court’s Jurisdiction can be broadly classified in to three categories as under:

1) Pecuniary

2) Subject Matter

3) Territorial

Pecuniary jurisdiction means jurisdiction based upon monetary limits. The eligibility of civil court’s to entertain suits is dependent on the value of the suits. When a case is filed, a claim is made. Each such claim is valued in monetary terms. Depending on the value of the claim, the court which would be competent to entertain the case is determined. If the claim is below Rs. 1, 00,000 the appropriate court to be reach to the civil judge(Senior Division) should be approached. Every case may be filed in the court of the lowest grade competent to try it. For e.g. a suit valuing above Rs. 5 lakh in Delhi

\(^{478}\) The Code s\textsection 19.
would have to be filed in the Delhi High Court and a suit up to Rs.5 Lakh in the District Court.479.

Jurisdiction of courts and the Information Technology Act 2000

Problem occurred when two persons from the different part of the world transact the business on the internet. Under such situation if one of the person wants to file a case in the court of law then the question arises as to where can he sue the another person with whom he transact the business on the internet. Traditional principles cover two aspects. One is the place where the defendant is residing and another where the incident occurred. However in the context of the Internet, both these are difficult to establish with certainty.

LEGAL PROVISIONS OF INFORMATION TECHNOLOGY ACT APPLICABLE IN THE DISPUTES OF JURISDICTION.

India has provided the legal remedy by way of particular law to control jurisdictinal problems a through Information Technology Act, 2000. Following provisions of the IT Act 2000 are invoked when a jurisdictinal dispute takes place. Since cause of action depends on the place wherefrom the parties communicates, interact and transact the business. Sub section (3),(4) & (5) of the section of 13 of the IT Act,2000 will be attracted for determining the place of cause of action. Let us discuss the above provisions as under:-

S.13 (3)480 Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business

Sec (4)481 the provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).

Sec (5)482 for the purposes of this section,-

479 Manikyam SITA . K. Dr., Cyber Crimes Law & policy perspectives, hind law house Pune 2009 edition p197
480 Sec.13(3) of ITAct2000
481 Sec.13(4) of ITAct2000
482 Sec.13(5) of ITAct2000
If the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business.

If the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business.

"Usual place of residence", in relation to a body corporate, means the place where it is registered.

Therefore from the above legal provisions of the IT Act 2000 it is clear that the place of dispatch and the receipt of electronic records and communications can be agreed upon between the interacting and transacting parties. However, where there is no agreement, it has to be presumed that the electronic record has been dispatched at the place of business. Where either or both of them do not have a place of business, the usual place of residence shall be considered as the place of business. For a company, the usual place of residence shall be the place where it is registered.

Since cause of action in Internet transactions depends upon the transactions between netizens, which is mainly through dispatch and receipt of electronic records, the above mentioned provisions of ITAct 2000 will be applicable.

It could be said that the aforesaid sub-section (3),(4) and (5) of section 13, being deeming provisions shall apply only for the purpose of the IT Act, whereas for the application of the concept of cause of action, under our civil law, only the places from where the parties actually interact by dispatch and receipt of electronic record shall be considered in all cases. This is still an unsettle thing and we have to wait till the High court and the Supreme Court takes any final decision.

**Section 75 of IT Act 2000**

This section is invoked for offences or contraventions committed outside India.

S.75 of the IT Act 2000 apply for offences or contravention committed outside India

(1) Subject to the provision of sub section (2), the provisions of this Act shall apply also to offence or contravention committed outside India by any person irrespective of his nationality

(2) For the purpose of sub-section(1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or

---

483 Section 75 of IT Act 2000
contravention involved a computer, computer system or computer network located in India.

The extra territorial application of the offence and whether such application can at all be permissible within the law of criminal jurisdiction. The wording of the section is such that it almost brings the whole word within the jurisdiction of the Indian court. In such case the question that arises “Can the Indian court exercise such a wide jurisdiction.

To understand the concept behind this section, we need to understand the “consequence” or “effect” theory, which has achieved good success in other leading jurisdictions around the world apart from India itself. The principle is that where an act is done abroad and criminal effect is produced here the crime is taken to be committed here. This theory has been described as the consequence theory.

The same principle is found in Section 179 of Code of Criminal Procedure. The section contemplates cases in which the thing done and its consequences happen in two different areas of jurisdiction and provides that in such cases the offence constitute by the act and the consequences may be inquired into or tried in either or the two areas. Thus if the jurisdiction for cross border killing or conspiracy or false representation is accepted, then with the Internet giving a much wider and global scope of committing crimes providing for a global jurisdiction to tackle crime and merely an extension of effect theory.

**Foreign judgment applicable in India.**

Indian civil Procedure Code provides that a foreign judgment is conclusive on matters directly adjudicated upon between the parties. But the same would have no applicability in India if a court of competent jurisdiction has not pronounced it, or it has not been delivered on the merits of the case. Further, it will have no applicability where it appears prima facie to be founded on an incorrect view of International law or refusal to Recognize The Law Of India in cases where such a law is applicable or where the proceedings are in violation of the Principles of Natural Justice i.e. where a fair hearing is not granted or the proceedings are based, or where the foreign judgment sustains a claim which is in breach of any Indian Law (Sec.13 CPC)

---

484 Manikyam SITA . K. Dr., Cyber Crimes Law & policy perspectives, hind law house Pune 2009 edition p197
International Conventions on Jurisdictional problem.
Following are the International Conventions on jurisdictional problem as under:-
1. European Convention on Cyber Crimes,
2. Convention on Cyber Crimes by G7 Groups
3. Convention on Cyber Crimes G8 groups etc.
In every convention jurisdictional problems have been highlighted and also respective cyber legislation of the states. The reason for doing all these to prevent the miscreants to take the benefits loop holes of law to avoid conviction in absence of jurisdiction clarity

LEGAL CASES RELATED TO JURISDICTION
1) SS Lotus Case (France v. Turkey)\textsuperscript{485} PCIJ Ser A (1927), No. 9
The Permanent Court of International Justice held that International law has imposed the restriction upon the countries that a country should exercise its jurisdictional power in any form in the territory of another country. Implied meaning of the jurisdictional in this case is territorial. One country should not intercept in the territorial jurisdiction in another country in no case unless a laissez-faire rule derived from the international custom or from a convention.”

2) United States v. Yunis\textsuperscript{486} 681 F Supp 896 (1988)
In this case the US District Court, District of Columbia held that passive nationality is offensive for a nation to insist that foreign laws are not sufficient to protect its citizens abroad. And therefore the every country has the jurisdiction over the crimes committed by their nationals abroad and each country has a legitimate interest to protect its nationals safety.

\textsuperscript{485}SS Lotus Case (France v. Turkey), PCIJ Ser A (1927), No. 9
\textsuperscript{486}United States v. Yunis, 681 F Supp 896 (1988)
3.4.7.(V) PROBLEMS RELATED TO EXTRA TERRITORIAL JURISDICTION AND EXTRADITION OF OFFENDERS JURISDICTION IN CASE OF CYBER CRIME:

To prosecute the cyber criminal in country by a national court, there must be some connection, between the regulating nation and the crime or criminal. The whole trouble with the jurisdiction of internet is there are so many parties involved in the crime are residing in various parts of the world who do not have real connection with each other. Then, if any party wants to file the petition against other, where can the party file the petition. Long-established requirement generally include two areas 1) The Place where the defendant resides, or 2) where the cause of action arises. Cyberspace has no geographical boundaries and it establishes communications with anybody who can have access to any website. Therefore a single transaction may involve the laws of at least three jurisdictions1) The laws of the state/nation in which the user resides, 2) The laws of the state/nation that apply where the server hosting the transaction is located, and 3) The laws of the state/nation which apply to the person or business with whom the transaction takes place.

Cyber Law dealing with Jurisdictional Problem in India: In India, the Information Technology Act, 2000 has been passed to deal with cyber crimes and there are specific forums in the Act which have the sole jurisdiction to deal with the cyber crimes mentioned in the Act.

Problem of Extra territorial jurisdiction & extradition of offenders

The problem facing by the law enforcement agencies when a citizen of some other country causes harm to citizens of a native country, let’s take for an example in India, though Information Technology Act, 2000 does have extra territorial jurisdiction but it’s very difficult to enforce it and exercise it. The problems relate to determination of place where the offence was committed and where several jurisdictions are equally competent. The Convention on Cyber crime has made cyber crimes extraditable offences. The offence is extraditable if punishable under the laws in both contracting parties by imprisonments for more than one year or by a more severe penalty. The Convention on Cyber crime has made the following criminal offenses extraditable as under:-
Bilateral extradition:
The word extradition as per Black Law Dictionary is as follows: “The surrender of a criminal by a foreign state to which he has fled for refuge from prosecution to the state within whose jurisdiction the crime was committed, upon the demand of the latter state, in order that he may be dealt with according to its law”

Extraditable Offences under Convention of cyber crime by G7 Groups

a) Offences against the confidentiality, integrity and availability of computer data and systems. These are as per the cyber crime convention i) Illegal access (Article 2), ii) Illegal interception (Article 3) iii) Data interference (Article 4), iv) System interference (Article 5) Misuse of devices (Article 6)

b) Computer related offences. These are as per the cyber crime conventions i) computer related forgery (Article 7) and ii) Computer related fraud (Article 8)

c) Content related Offences. This is as per the cyber crime convention offences related to child pornography (Article 9)

d) Offences related to infringements of copyright and related rights. These are as per cyber crime convention i) Offences related to infringements of copyright and ii) related rights (Article 10) Attempt and aiding or abetting (Article 11)

Bilateral Extradition treaties: India is still not a signatory to the Cyber Crime Convention and the bilateral extradition treaties, which it has signed with around 50 countries so far, do not mention ‘cyber crime’ as extraditable offences. A CBI Special Judge, New Delhi, Talwant Singh at a seminar on 5/10/2012 states that India is yet to sign the extradition treaties with other countries, he also added that till date, we do not have a single treaty with any other country to extradite a cyber criminal to be brought to India. He said India has physical boundaries in terms of its geographic location with other countries, but there was no such boundary in cyber world and it is not yet defined. We have to protect our cyber boundaries also.

Indian Situation: Under the Information Technology Act, 2000, Section 75 of the Act, deals with extraterritorial application of the law, the section states that the provisions of the Act will apply to: Any person irrespective of nationality and an offence or
contravention committed outside India. The Act has therefore adopted the principal of
universal jurisdiction to cover both cyber contraventions and cyber offences. Though
S.75 provides for extra-territorial operations of this law, but they could be meaningful
only when backed with provisions recognizing orders and warrants for Information
issued by competent authorities outside their jurisdiction and measure for cooperation
for exchange of material and evidence of computer crimes between law enforcement
agencies.
Moreover, it is important to note that India at present does not have a proper extradition
law to deal with crimes that have been committed over the Internet. To address this
issue, India should become a signatory to the Convention of cyber crimes treaty and
should ratify it. Recently India has signed cyber crimes related treaties with 19 countries
to attain legal compatibility.
Whatever stated in the foregoing paragraphs it will be fair enough to say that the
measures taken by the Government of India are not sufficient to curb and control cases
of extraterritorial jurisdiction. Though the Government has provided the statute to deal
beyond the territorial boundaries but it has not given any framework for its execution.
Unless there is no international co-operation and legal harmony between the countries
there is no use of drafting such legal provision to control the cyber crime are not
effective.

LEGAL CASES RELATED WITH EXTRADITION
1) Daya Singh Lahoria v. Union of India [487](2001) 4 SCC 516

In this case the provisions of The Extradition Act, 1962; Section 21 provides that if a
person is brought into India under an extradition decree, he cannot be tried in respect of
an offence, which does not form part of the decree. The person can be tried only for the
offences mentioned in the Extradition decree and for no other offences. The courts in
India have certainly no jurisdiction to try such person for any other offence.
The case of the prosecution was that the appellant herein along with his wife Suman
Sood alias Kamal Jeet Kaur fabricated Registration Certificate for purchasing several
vehicles in order to carry out conspiracy of kidnapping and abducting one Rajender
Mirdha, son of Shri Ram Niwas Mirdha to exert pressure on the Government of India to

release one Devendra Singh Bhullar, an alleged Khalistani terrorist who was being held in custody by the police. It was also alleged that the appellant was found to be in possession of prohibited arms and ammunition allegedly recovered from House No. B-117, Model Town, Ashok Nagar during police raid where the appellant was staying. Initially, prosecution was launched in the Designated Court at Ajmer since the provisions of TADA were also invoked. The appellant herein, however, challenged his prosecution under TADA. This Court upheld the challenge since the prosecution of the accused could only be maintained in accordance with the Extradition Treaty and the Decree of Extradition under which the accused were extradited by the United States of America to India. Thereafter, the case was registered as Sessions Case No. 27 of 2003 under the Indian Penal Code and also under the Explosive Substances Act, 1908. The trial Court, after considering the evidence on record, convicted accused No.1 (appellant herein) as under: Under Section 420, 468 and 471IPC : to 7 years R.I. and a fine of Rs.500 Under Section 4 of the Explosive Substances Act: to 7 years R.I. and a fine of Rs.500/-

The learned counsel of the appellant submitted that Extradition Treaty of 1931 between United States of America and Great Britain and the Extradition Order passed by the American Court on June 11, 1997, the appellant could not have been prosecuted in Indian Court and the trial of the appellant was without authority of law. On merits also, no case had been made out by the prosecution. In the light of the finding recorded by us in the cognate matter, this appeal is, more or less, academic and has become infructuous in view of the following circumstances;

(i) the appellant has been convicted for an offence punishable under Section 364A, IPC and has been ordered to undergo sentence of imprisonment for life and we have upheld the said order; and
(ii) in the present appeal, the appellant has challenged his conviction and sentence whereby he has been ordered to undergo imprisonment for seven years. The appellant has remained in jail for seven years and the said period is over.

16. For the foregoing reasons, the appeal deserves to be disposed of and is accordingly disposed of without entering into merits of the case.
2) Hans Muller of Nuremberg v. Superintendent Presidency Jail, Cal.\(^{488}\) (AIR 1955 SC 367)

The petitioner, Hans Muller, who is not a citizen of India, and who is said to be a West German subject, was arrested by the Calcutta Police on 18th September, 1954 and was placed under preventive detention. The order was made by the West Bengal Government under Section 3(1) of the Preventive Detention Act of 1950 (Act 4 of 1950) on the ground that his detention was “With a view to making arrangements for his expulsions from India”.

The petitioner contended that his detention was invalid for the following, among other, reasons:

1. Because Section 3(1)(b) of the Preventive Detention Act, the section under which the order was made, is ultra virus the Constitution on three grounds —
   a. that it contravenes Articles 21 and 22;
   b. that it contravenes Article 14, and
   c. that it was beyond the legislative competence of Parliament to enact such a law;

The High Court decided against the petitioner on all points and dismissed the petition on 10-12-1954. He thereupon made the present petition to this court on the same grounds, presumably under Article 32 of the Constitution. It was filed on 10-1-1955.

The conclusion of the court was that the Foreigners Act is not governed by the provisions of the Extradition Act. The two are distinct and neither impinges on the other. Even if there is a requisition and a good case for extradition, Government is not bound to accede to the request. It is given an unfettered right to refuse. Section 3(1) of the Extradition Act says — “The Central Government may, if it thinks fit”.

Therefore, if it chooses not to comply with the request, the person against whom the request is made cannot insist. The Court held that even if there is a requisition and a good cause for extradition, the government is not bound to accede to the request,

\(^{488}\) Hans Muller of Nuremberg v. Superintendent Presidency Jail, Cal., AIR 1955 SC 367
3.4.8(VI) EVIDENCE RELATED PROBLEMS IN CYBER CRIME CASES

The expansion of computers has created a number of problems for the law. Legislative rules required various records likewise paper records, of signed records, of original records. The law of evidence customarily depends on paper records and these paper have to be proved in the court though oral deposition and other kinds of physical objects. As more transactions are carried out by electronic means, it becomes pertinent that evidence of these transactions should be available to display the legal rights that flow from them.

Most electronic records are generally admitted in the court. Therefore in this electronic era there was a growing demand by the users to substitute the hand-written signature in the electronic environment, granting integrity, confidentiality and legitimacy of information and documents.

Definition of Digital Evidence

1) The digitization and emerging use of ICT has a huge impact on procedures for the collection of evidence and its use in court.489

2) The United Kingdom (UK) Police and Criminal Evidence Code define digital evidence as “all information contained in a computer”490.

3) Prior to the amendment by ITAct, 2000, the definition of ‘Evidence’ in section 3 of the Indian Evidence Act, 1872 was as follows491.

“Evidence” means and includes:

(1) All statements which the court permits or requires to be made before it by witnesses, in relation to matters of fact under enquiry, such statements are called oral evidence.

(2) All documents produced for the inspection of the Court, such documents are called documentary evidence

4) The aforesaid definition has now been amended by the IT Act, 2000 which reads as 492.

(1) All statements which the court permits or requires to be made before it by

---

490 UK) Police and Criminal Evidence Code
491 Section3 of the Indian Evidence Act, 1872
492 IT Act 2000
Witnesses, in relation to matters of fact under enquiry; such statements are called oral evidence.

(2) All documents including electronic records produced for the inspection of the court, such documents are called documentary evidence.

**Types of computer-generated evidence:**

Those are of three kinds namely

1) Real Evidence
2) Hearsay Evidence and
3) Derived Evidence

**1) Real Evidence:** - Real evidence is defined as evidence of a tangible nature from which the tribunal of fact can derive information by using its own senses⁴⁹³.

Real evidence has been described as the most satisfactory kind of evidence since, save for identity or explanation, neither testimony nor inference is relied upon. Unless its genuineness is in doubt, the thing speaks for itself.⁴⁹⁴

For example, if a bank computer automatically calculated the processing fees, incidental charges and monthly interest/overdue interest/penal interest due from a borrower of the bank, such types of the transactions in the account and outstanding debit balance, this is termed as the part of real evidence.

**2) Hearsay Evidence:** - Hearsay evidence is evidence given by a witness in court of a statement made by some other person out of court, when such evidence is tendered to prove the truth of the statement⁴⁹⁵. Under common law, hearsay evidence was generally inadmissible; but in civil proceedings this rule was abolished in the UK by the Civil Evidence Act 1995, which provides for the admissibility of hearsay evidence subject to statutory safeguards, and preserves a number of common law exceptions to the rule against hearsay⁴⁹⁶.

**3) Derived Evidence:** - This consists of real evidence and the information feed by the human being in the computer to form a combined record. Derived evidence is by and
large treated as hearsay evidence also. For example figure in the debit balance column of a bank statement of loan account processing fees, incidental charges and monthly interest/overdue interest/penal interest due from a borrower of the bank as it is derived from real evidence i.e. automatically generated and hearsay evidence individual deposits of cheques and pay-in entries in the loan/advances/ cash credit accounts.

IDENTIFICATION PROCEDURES OF EVIDENCE IN THE CYBER CRIMES

There is a prominent difference between the real world and cyber world. Evidence is passing through the following stages:

1) Detection of Evidence
2) Gathering & collection of evidence
3) Storage of the evidence and
4) Exhibition of evidence before the court.

There is a difference in all the stages in respect of the detection of evidence to exhibition of evidence before the court. It is pertinent to note that the investigation officers must understand the different elements of the evidence right from the stage of collection of the evidence to the presentation of the evidence before the court. The judiciary should be well versed with the computer evidence produced before the judges. In virtual world to trace the evidences in the tangible form like finger prints, weapon of crime, blood stain etc. is not so easy as compared to collection of evidence in real world. The computer forensics is achieving importance in the investigation departments, corporate world, government departments’ etc. Let us discussed some of the problems those are connected with the course of cyber evidence detection, gathering, storage and exhibition before the court.

It is very much difficult to regenerate the information from the computer system which was intentionally deleted by the miscreants. But with the help of the forensics experts the deleted information which was intentionally deleted can be regenerated. Therefore it is very much essential to report to the law enforcement agencies by the victim as early as possible. The computer evidence generated by the forensics expert should be preserved carefully in such a manner that there should be no diminish of value evidence

---

497 Explanatory Report to the Council of Europe Convention on Cybercrime
as it is stored in a very miniature form. Therefore the timely help of the forensics expert 
can assist to collect evidence from the computer system within shortest possible time. 
Cyber evidence may be in the physical or logical form. Physical evidence can be traced 
easily by its nature and the investigator has to visit the site of crime and search the 
required evidence and possessed into his custody like computer hardware, which may 
constitute main frame computers to pocket sized personal assistants, floppy diskettes, 
electronic chips etc.

**Admissibility of the Evidence:** Recording of evidence for satisfying the object of the 
Evidence Act that the evidence be recorded in the presence of the accused. Since 
computer generated evidence is a recent development, till date Indian law has not 
issued the guidelines in this regard. The UK and USA law are referred in this regard. 
References to the UNCITRAL Model Law on Electronic Commerce are also made 
With the enactment of the IT Act, the evidence in the electronic form is recognized by 
law. In place of paper documents and signatures, evidence in the form of electronic are 
admissible in court and may be proved. But for this originals to be presented in the 
court. We must admit that electronic records can be easily tampered and could not be 
authenticated in a perfect manner. Therefore acceptance of electronic evidence should 
be depending on case to case basis.

**Maintenance of Records:** Section 4 of the Bankers’ Books Evidence Act, 1891, 
provides that a certified copy of any entry in a banker’s book shall in all legal 
proceedings be received as a prima facie evidence of the existence of such an entry. 
The Banking Companies (Period of Preservation of Records) Rules, 1985 promulgated 
by the Central Government requires banking companies to maintain ledgers, records, 
books and other documents for a period of 5 to 8 years. A fear has been expressed as 
to whether the above details of the transactions if maintained in an electronic form will 
also serve the above purpose. The Group is of the considered opinion that that this has 
been adequately taken care of by Section 7 and Third Schedule of the Information.
PROBLEM RELATED WITH RECORDING OF EVIDENCE

1) Lack of training to the Computer Forensic Expert

Computer generated evidence which is popularly known as digital evidence is a new phenomenon in India and it is the new class of evidence and the field is budding rapidly. The detection, search and seizure is the difficult task therefore the procedures for searching, seizing and analyzing digital evidence there is an urgent need of scientific reliable procedures for collection and preservation of evidence and for that purpose training must be provided to computer forensic expert.

2) Lack of recording mechanisms that accurately distinguish between online and offline crime.

Indian police is not expert and trained to identify the crime as a cyber crime. Police generally recorded crime does not make a distinction between online and offline crimes, making it complicated to recognized as cyber crimes. Police record crime in accordance with the provisions of the Cr.P.C, and Indian Evidence Act, 1872 which set out that the crime to be recorded as per the set rules determined by the law. Police recorded crime does not generally distinguish between online and offline offences and not as per the provisions of Information Technology Act 2000 and Information Amendment Act 2008.

3) Lack of global harmonization of legal standards, in the area of digital evidence at international level.

Network technologies and computer are used worldwide and the problems related to the acceptability of digital evidence in court are similar though the statutes of the countries in globe are different. Obligatory legal standards for the digital evidence have not been put into practice at international level. Only few countries including India have so far on track to update their legislations to facilitate courts to deal directly with digital evidence. Though there are various criminal laws and procedural instruments to combat with cyber crime but there is a lack of global harmonization of legal standards, in the area of digital evidence at international level.

4) Cyber crime is global in nature. It is not constrained by national boundaries.

Cyber crime offences and their perpetrators may originate outside of the national jurisdiction they impact on. For example, a computer virus may be written in the Far East but cause damage in Europe, or a downloading site may be located in Russia but
accessed in the UK. This presents as many problems for accurate measurements of cyber crime as it does for identifying offenders and bringing them to justice – particularly where other jurisdictions have different legislation.

5) *Cyber crime can be undertaken on a large scale, potentially resulting in a relationship between victims and offenders that is very different to ‘offline’ crime.*

Unlike most traditional crimes, cyber crimes can be undertaken on a large scale and one offender may be linked to a vast number of smaller crimes (for example, a botnet which is able to send out masses of phishing emails). In most of these situations the offender would be perceived as largely anonymous by the victim. Furthermore, when aggregated, these smaller offences may still create a substantial return for the offender. Data collection and recording in this area will therefore face particular challenges in linking together seemingly isolated incidents. Part of the work of the CBI, State Intelligence Buero and EWS seeks to draw together the linkages and commonalities between seemingly isolated incidents into ‘packages’ of intelligence for local police and other partner agencies to investigate.

6) *Flimsy Nature of Digital Evidence*

Digital data is flimsy in nature and can be easily altered or deleted. Therefore digital evidence is disquieting in nature. Without technical expertise and a slight mistake may be resulted into loss of evidence.

7) *Under-reporting of cyber crime, from both the public and business and lack of awareness that some cyber incidents are actually crimes.***

Cyber crimes are under-reported; for example, recent findings from the National Crime Record Bureau (NCRB) report 2012 suggest that cases reported under IT Act 2000 are considerably lower than for other crime types.

Under-reporting may occur for a number of reasons:

a) perceptions that the police will not/cannot do anything about online crimes;
b) not knowing where to report;
c) reporting to other bodies such as banks or internet service providers;
d) perceptions that cyber crimes are not ‘real’ crimes like, for example, vehicle theft or burglary;
e) victims not realizing or perceiving themselves as victims, for example, because a bank has refunded lost money, or being unaware that malware has infected their computer and stolen their personal details; and

f) some victims simply being too embarrassed to come forward, for example, regarding common scams.

8) Low cost of storage of documents in a digital forms

The problem of detection, search and seizure of the digital evidence is the herculean task for investigators. It is because the low costs of storage of digital documents as compared to the storage of physical documents are giving rise to an increasing number of digital documents. Though there is an availability of facility to automatic search to identify the relevant digital evidence on a storage device. But a storage device carry huge documents is a herculean task for computer forensic officer to search and detect the digital evidence.

9) Dependency on the expert of Judges, Lawyers and prosecutors

Lawyers, prosecutors and Judges are mostly depends on the expert of digital evidence as analysis and evaluation requires special skills and technical understanding which is usually not the part of the education of lawyers, prosecutors and Judges.

10) Internet user may left the footprints of evidence while working on the Internet

Internet users left the traces while working on the internet, This is the useful source of digital evidence in investigating the crime in the cyber space.

11) Problems with Certification and Internet-based evidence

The problem with certification created by Internet evidence, can be classified in to two categories i.e 1) Continuity of Access Evidence and 2) False Identification – Spoofing. Though the evidence is admitted, but it can be challenged on a number of reasons like lack of integrity, lack of truthfulness and lack of relevance to the issue. The opponent has to prove such shortcomings as the burden of proof lying upon him.

LEGAL PROVISIONS FOR EVIDENCE RELATED TO CYBER CRIME


In 2000, the Law Ministers of Small Commonwealth Jurisdictions decided to establish a working group to develop model legislation on electronic evidence. The main
comparative law analysis finding of the study group was that, with regard to the admissibility of digital evidence, the reliability of the system by which the digital evidence was created is more important than the document itself.

2) Position in India:- IT Act 2000, ITA A 2008 and Indian Evidence Act, 1872

I) Admissibility of Electronic Record under Information Technology Act, 2000

The Information Technology Act granted a comprehensive permission for records produced as evidence should not to be denial to the legal effect of the document being produced in the electronic form as long as they are available for future response. The Act amends the definition of ‘evidence’ to include “all documents including electronic records produced for the inspection of the court.”

Further, the IT Act provides that “where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is-

(a) Rendered or made available in an electronic form; and

(b) Accessible so as to be usable for a subsequent reference.

It also describes the manner in which the electronic document is to be proved in law.

II) Authentication of electronic records/ Digital/Electronic signatures

a) Digital Signatures :-A combined reading of Section 2(p) and sub-sections (1) and (2) of Section 3 of Information Technology Act 2000, makes it clear that in terms of the Act an electronic record may be authenticated by affixing ‘digital signature’ and if a party wants to authenticate the electronic record by affixing digital signature, the electronic method or procedure for affixing digital signature shall be asymmetric crypto system and hash function.

b) Electronic Signature: - Information Technology (Amendment) Act, 2008 has brought in the concept of ‘electronic signature’ and has defined it as under:

“electronic signature means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second Schedule and includes digital signature.”

---

498 Indian Evidence Act, 1872; Section 3
499 The Information Technology Act, 2000; Section 4
500 Section 65 A and section 65 B of the Indian Evidence Act, introduced by the IT Act, 2000 amending provisions
Section 3A of Information Technology (Amendment) Act, 2008 provides as under:

**Electronic Signature:** (1) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (2), a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which--
(a) Is considered reliable; and
(b) May be specified in the Second Schedule.”

**Proof of Digital Signature:** Under section 36 Information Technology (Amendment) Act\(^{501}\), a Certifying Authority while issuing a Digital Signature Certificate shall certify, *inter alia* that,-

(ca) the subscriber holds a private key which is capable of creating a digital signature;
(cb) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the subscriber

**Section 42 of the Information Technology (Amendment) Act\(^{502}\)** requires every subscriber to exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure. Further, if the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber is required to communicate the same without any delay to the Certifying Authority in such manner as may be specified by the regulations. It has been clearly laid down in the explanation to section 42(2) of the Act that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised

**Under Section 67A of Indian Evidence Act, 1872\(^{503}\),** the Court shall presume, unless contrary is proved, that the information listed in an Electronic Signature Certificate (which includes digital signature certificate) is correct. A combined reading of the above provisions makes it clear that the court shall presume that the subscriber has the private key and that the public key listed in the digital signature certificate may be used to verify the digital signature affixed by using that private key. Though this is a rebuttable presumption, it may reasonably be concluded that the subscriber has little chance of successfully challenging the contents of an electronic record authenticated by using

---

\(^{501}\) section 36 Information Technology (Amendment) Act

\(^{502}\) Section 42 of the Information Technology (Amendment) Act

\(^{503}\) Section 67A of Indian Evidence Act
digital signature. Under section 73A of the Indian Evidence Act, in order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct--

“(a) That person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;
(b) Any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person.”

This makes proof of digital signature easy.504

III) Binding nature of other Electronic Records505

The question that arises for consideration is whether a party may be bound by the transactions entered into through electronic means (whether through ATMs, Internet or otherwise) though the electronic records in question are not authenticated by using digital/electronic signature.

Section 65B (1) of Indian Evidence Act, 1872 reads as under:

“1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence or any contents of the original or of any fact stated therein of which direct evidence would be admissible.”

It is thus clear that electronic records may be proved in courts even though they are not authenticated by using digital or electronic signature if the conditions mentioned therein are satisfied. The difficulty in proving the various conditions set forth in sub-sections (2) and (3) of section 65B of Indian Evidence Act is ameliorated to a great extent by sub-section (4) thereof under which the certificate of a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities

504 Report & Recommendations of the working group of information security, electronic banking technology, risk management and cyber fraud published by RBI on January 2011
505 ibid
(Whichever is appropriate) shall be evidence of any matter stated in the certificate. The information stored in the central computer systems of a departmental store was relied on to hold a person guilty of theft. The evidence of store detective that there was no evidence of malfunctioning of central computer was accepted. It may therefore be concluded that it is possible to prove electronic records in courts even if the electronic records are not authenticated by digital or electronic signatures

IV) Examiners of Electronic Evidence

Section 79A of the Indian Evidence Act which reads as under.

Sec79A-Central Government to notify Examiner of Electronic Evidence.-- The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the Official Gazette, any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

Explanation.-For the purposes of this section, "electronic form evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines." As the courts are not equipped to deal with the technological issues that may arise in evaluating the evidentiary value of electronic records, it is recommended that Central Government should specify sufficient number of agencies under section 79A of the Act to assist courts in arriving at a decision on the evidentiary value of electronic records irrespective of whether digital or electronic signature is affixed or not

LEGAL CASE RELATED TO ELECTRONIC EVIDENCE


These Appeals are against a Judgment of the Bombay High Court dated 23rd/24th April 2001. The question for consideration is whether in a criminal trial, evidence can be recorded by video conferencing. The High Court has held, on an interpretation of Section 273, Criminal Procedure Code, that it cannot be done. Criminal Appeal (arising out of SLP (Criminal) No 6814 of 2001) is filed by the State of Maharashtra. Criminal Appeal (arising out of SLP (Criminal) No 6815 of 2001) is filed by Mr. P. C. Singhi, who was the complainant. As the question of law is common in both these Appeals, they are being disposed of by this common Judgment. In this Judgment parties will be referred to
in their capacity in the Criminal Appeal (arising out of SLP (Criminal) No 6814 of 2001). Mr. P. C. Singhi will be referred to as the complainant.

The complainant's wife was suffering from terminal cancer. It is the case of the prosecution that the complainant's wife was examined by Dr. Ernest Greenberg of Sloan Kettering Memorial Hospital, New York, USA, who opined that she was inoperable and should be treated only with medication. Thereafter the complainant and his wife consulted the Respondent, who is a consulting surgeon practicing for the last 40 years. In spite of being made aware of Dr. Greenberg's opinion the Respondent suggested surgery to remove the uterus. It is the case of the prosecution that the complainant and his wife agreed to the operation on the condition that it would be performed by the Respondent. When the stomach was opened ascetic fluids oozed out of the abdomen. Dr. A. K. Mukherjee contacted the Respondent who advised closing up the stomach. Dr. A. K. Mukherjee accordingly closed the stomach and this resulted in intestinal fistula. Whenever the complainant's wife ate or drank the same would come out of the wound. The Maharashtra Medical Council has, in an inquiry, held the Respondent guilty of negligence and strictly warned him.

These Appeals are against a Judgment of the Bombay High Court dated 23rd/24th April 2001. The question for consideration is whether in a criminal trial, evidence can be recorded by video conferencing. The High Court has held, on an interpretation of Section 273, Criminal Procedure Code, that it cannot be done. Criminal Appeal (arising out of SLP (Criminal) No 6814 of 2001) is filed by the State of Maharashtra. Criminal Appeal (arising out of SLP (Criminal) No 6815 of 2001) is filed by Mr. P. C. Singhi, who was the complainant.

As the question of law is common in both these Appeals, they are being disposed of by this common Judgment. In this Judgment parties will be referred to in their capacity in the Criminal Appeal (arising out of SLP (Criminal) No 6814 of 2001). Mr. P. C. Singhi will be referred to as the complainant.

Recording of evidence by video conferencing also satisfies the object of providing, in Section 273, that evidence be recorded in the presence of the Accused. The Accused and his pleader can see the witness as clearly as if the witness was actually sitting before them.
Accordingly the impugned judgment is set aside. The Magistrate will now proceed to have the evidence of Dr. Greenberg recorded by way of video conferencing. As the trial has been pending for a long time the trial court is requested to dispose off the case as early as possible and in any case within one year from today. With these directions the Appeals stand disposed of. The Respondent shall pay to the State and the complainant the costs of these Appeal.

2) King v. State ex rel. Murdock Acceptance Corp., 222 So. 2d 393 (Miss., 1969)

in the American case of King v. State ex rel. Murdock Acceptance Corp., 222 So. 2d 393 (Miss., 1969), the issue was whether a print out satisfied the requirement of being an original record. It was held that the printouts were admissible evidence of a permanent record on magnetic tape. This was because of the obvious fact that records stored on magnetic tape were unavailable and useless except by means of printouts.

*****