CHAPTER - II
CHAPTER-II

Progress of Banking in India, Meaning and Concept of E-Banking, Meaning and Concept of Cyber Crimes in Banking and Cyber Crime Offenses related with Banking

Banking is the oldest form of trade and business in the world and has its survival from ancient times in India. The last decade of the previous century [1990 to 2000] acknowledged as “Information Technology Revolution Decade”. These technological improvements mainly in information technology have made the changeover possible from paper to paperless transactions in banking. Therefore, traditional banking is shifted to electronic banking popularly known as e-banking.

“Scientific inventions, when put into wrong use by mankind, give rise to social problems, in their turn, lead to controversies and conflicts. In the long run, these conflicts often assume a legal dimension with aim to provide remedies to parties”. Information technology furnishes as an apt example of what has been stated above.  

Growth in Information Technology has also contained the various challenges which have to face by the society. The cyber threat landscape is also changing over the years and needs to be factored in while considering mitigating measures  

In the age of information technology the swift expansion of, telecommunications, computers and other technologies has led to new forms of worldwide crimes known as “Cyber Crimes”. Cyber crimes have practically no boundaries and may affect every country in the world. Mounting Cyber crimes across the world is a very stern warning in the up-coming time and produces one of the most complicated challenges before the law enforcement machinery. 

39 Dr. P. M. Bakshi and Dr.R.K.Suri” Handbook of Cyber and E-commerce Laws” by Pentagon 2002 p1
2.1. PROGRESS OF BANKING IN INDIA

2.1.1 GENERAL HISTORY OF BANKING
The Banking industry is one of the oldest in the world. Banking originated about 4000 years ago in places such as Babylon, Mesopotamia and Egypt where grain & other valuable commodities were stored and receipts given as proof of sale on purchase.

ORIGIN OF THE WORD “BANK”
The word bank was borrowed in Middle English from Middle French banque, from Old Italian banca, from Old High German banc, bank "bench, counter". Benches were used as desks or exchange counters during the Renaissance by Florentine bankers, who used to make their transactions atop desks covered by green table cloths. There are the different opinions on the origin of the world “bank”. According to different opinions, the word “BANK” itself is derived from the word “bancus” or “bankue” that is a bench. The Jews in Lombardy were termed as early bankers those were transacting their business on benches in the market place. This opinion is, however, rejected by Henry Dunning Macleod, a Scottish economist, on the ground that “The Italian money changers as such were never called “Banchieri” in the Middle Ages. Others opinion in this regard is that the word “bank” is originally derived from the German word “back” meaning a joint stock fund. When the Germans captured a great part of Italy, this word “bank” was later Italianized into “banco”. M.I.Tannan supported this view. But “whatever be the origin of the word “bank,” as Professor Ramchandra Rao says (Present-Day Banking in India, 1st edition, p.88) “It would trace the history from the Middle Ages.”

EARLY BANKING SYSTEM
The History of Banking is very old and we find its roots at about 2000 BC within the boundaries of Assyria and Babylonia where the banks which were the first of its kinds

---

44 M.I.Tannan” Banking Law and Practice in India” 18th edition 1990, India Law House, New Delhi, p2
and were controlled by the merchant of ancient world. These banks granted grain loans to farmers and traders those who were carrying goods between the cities. In ancient Greece and during the regime of Roman Empire, the temples of Babylon were used as banks and such great temples as those of Ephesus and of Delphi made loans. Those temples were the most powerful of Greek banking institutions during those days. During these periods two important innovations were occurred those were the accepting of deposits and the changing of money.

The Greeks organize the State Owned Banks while Romans did not organize their State owned Banks; the conduct of their private banking earned & created the public confidence in their system. With the end of the civilization of antiquity, banking system deteriorated for a period of so many centuries into a system of financial change. In the middle of the 12th century, some banks were established at Venice and Geneva, due to growing requirement of the society. During the 14th Century, some of the famous bankers throughout Europe were Bardi, Acciajuoli, Peruzzi, Pitti and Medici. During the 15th century the Peruzzi Family opened various branches in Europe & played a notable role in financing to “Christopher Columbus” and “John Cabo” for some of their early voyages of discovery to America.

The predecessors of modern banks were frequently licensed for an explicit purpose. For example, the Bank of Venice (1171) and the Bank of England (1694) were chartered in relation with loans to the government; the Bank of Amsterdam (1609) was established to receive deposits of gold and silver. There was a rapid growth of all the way through the 18th and 19th century, supplementing the growth of the industries and trade. Each country of the globe developed the individual structure of banking peculiarly suited to its economic and social life.

The importance of banking system was recognized by the people because they had realized the value of money in their life. The importance of banking system has its origin in the earlier centuries only.

---

45 TannanM.I.” Banking Law and Practice in India” 18th edition 1990, India Law House, New Delhi, p3
47 G. G. Munn, Encyclopedia of Banking and Finance (8th rev. ed. 1983);
2.1.2 BACKGROUND OF BANKING IN INDIA

From the ancient times, the banks & bankers are essential pillars of the Indian society. Previously concept of banking was not present in Indian society due to independence & self support was the customary law. But when division of work was introduced in the society, there were complicatedness in the matter of exchange. Due to this problem, Indian society understood how to make use of money. Existence of money economy is not possible without banking institution. ⁴⁸

There are number of evidences to show that India was not an unfamiliar to the notion of the banking. “Loans and usury were well understood in those days and Rishis (who, we should always remember, were worldly men in those days and not solitary person or hermits or anchorites) occasionally laments their state of indebtedness with the simplicity of primitive times”.⁴⁹

To pay off the debt was called as “Rnam-Sam-m”. There are number of citations available in respect of contract of debts were executed without intention of payments. From the above it is evident that as early as the Vedic period the accepting and pay off the credit in one or other form were in existence. However, the changeover from money lending to banking must have occurred before Manu, who has devoted a special section to the subject of deposits and pledges, where he says, “A sensible men should deposit his money with a person of good family, of good conduct, well acquainted with the law, veracious, having many relatives wealthy and honorable(Arya)⁵⁰.

In respect of Policy of loans and Rates of Interest were governed by the rules of Manu. Accordingly, the banking business was carried out in ancient India.⁵¹ There are many strotras in the work of Gautama, Brihspati and Kautilya regarding the regulation of the interest⁵². In those days banking meant largely money lending, financing to kings for their war. Bankers in India were highly respected as very important member of the community in Government, as well as in society. Banker was often consulted also in financial matters of State as well as on the other matters. When uncertainty, insecurity

⁴⁸ TannanM.I. “Banking Law and Practice in India” 19th edition 1990, India Law House, New Delhi,p⁸
⁴⁹ Dutt R.C., “Civilization in Ancient India by” Vol.1, revised edition p³⁹.
⁵¹ per say Sir Richard Temple’s lectures: Journals of the Institute of Bankers, Vol2,
was prominent aspect of the time disturbed days of civil wars, the Banker was the most trusted person the only shelter in money matters. The Indian banker was extremely admired and considered as commendable example of commercial integrity.\textsuperscript{53}

There were some transactions very popular in Indian Banking System which has been accepted since long time such as:

**The Hundi:** - The word hundi is said to be derived from the Sanskrit root "\textit{hund}" meaning to collect. Its derivation expresses the purpose for which originally instruments were used. The Indian Bankers always enjoyed the public confidence in banking in vogue. This can be understood from the fact that hundis (Inland bill of exchange) are in existence from the days of the Mahabharata. Among the Hindus, the banking was restricted to the issue and discount the bill of exchange, money lending and money changing. Very often banking was also carried on together with dealings in grains, cloths etc. The role of the banker pivotal in the commercial market as well as in agricultural field. Hundis were effectively used for transfer of funds at a fairly distant places \textsuperscript{54}

**Usury:** - In Bengal, money were frequently lent to farmers at high rate of interest forty, and sometimes, even at sixty percent, per annum, while the standing crop was mortgaged for repayment of the loan. Usury was widely customary in India.\textsuperscript{55}

**The Money Lending:** - The early Indian bankers had comparatively a little deposit or discount business, or dealings in other people’s money, which is the unfailing characteristic of modern banking. Therefore he may be called a money lender rather than a banker.\textsuperscript{56}

\textsuperscript{53} Tannan M.I. “Banking Law and Practice in India” 18\textsuperscript{th} edition 1990, India Law House, New Delhi, p\textsuperscript{9}

\textsuperscript{54} ibid\textsuperscript{10}

\textsuperscript{55} ibid

\textsuperscript{56} ibid
2.1.3 THE JOURNEY OF BANKING IN INDIA [1786-2013]

The journey of Indian Banking System from 1786 to 2013 can be segregated into seven distinct phases as mentioned below:

<table>
<thead>
<tr>
<th>Phase I (1786-1934)</th>
<th>Early Phase of Indian Banking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phasell (1935 -1968)</td>
<td>Pre-nationalization phase of Indian Banking</td>
</tr>
<tr>
<td>Phaselll (1969 -1979)</td>
<td>Post-nationalization phase of Indian Banking</td>
</tr>
<tr>
<td>PhaseIV ( 1980-1990)</td>
<td>Preparatory phase of E-Banking in India</td>
</tr>
<tr>
<td>Phase V (1991to2000)</td>
<td>Emergent phase of E-Banking in India</td>
</tr>
<tr>
<td>Phase VI (2001-2008)</td>
<td>Transitional phase of E-Banking in India</td>
</tr>
<tr>
<td>Phase VII (2009-2013)</td>
<td>Matured phase of E-Banking in India</td>
</tr>
</tbody>
</table>

2.1.3 (A) PHASE-I (1786 -1934)

Early phase of Indian Banking

Phase I is known as “The Early Phase of Indian Banking”. It describes the progress of banking from establishment of 1st joint stock bank. In the present sense, foot prints of Indian banking can be traced in the last decades of the 18th century. East India Company is pioneer in establishment of banking during the early phase banking in India. This phase witnessed the progress of Indian banking in the following manner:

The Rise of Joint Stock Banks in India: - Banking in India set in motion in the last but one decade of the 18th century. The first bank “The General Bank of India” was established in the year 1786 when Warren Hastings was the Governor General of India. “Bank of Hindustan” was founded in 1790. “The State Bank of India”, countries largest & oldest bank was derived from the “Bank of Calcutta” established on 2nd June, 1806, which was renamed as “Bank of Bengal” on 2nd January 1809. In 1862, Bank of Bengal was amalgamated in “Dacca Bank” which was established in 1846. Three “Presidency Banks” were established under charters from the “British East India Company” namely 1) Bank of Bengal ,2) Bank of Bombay established on 15th April, 1840 and 3) Bank of Madras on 1st July 1843. The three banks were amalgamated as “The Imperial Bank of India” on 27th, January 1921. The Reserve Bank of India, being The Central Bank of India, took over the control of The Imperial Bank of India and the Imperial Bank of India was merged on 30 April 1955 as the State Bank of India. Indian merchants in Calcutta
established the Union Bank in 1839. Due to “Economic Crisis of 1848-49”, the bank was failed in 1848. In 1865, "Allahabad Bank" was established which is the oldest Joint Stock bank in India.
In the year 1860, foreign banks also started opening of their branches particularly in Calcutta. In 1860 “The Comptoir d’ Escompte de Paris” opened its branch in Calcutta.
In the year 1869, Hong Kong-Shanghais Banking Corporation (HSBC) established itself in Calcutta. Mainly due to trading activities of the British Empire Calcutta became the most dynamic trading port in India and in turn so became a banking center. The Punjab National Bank was established in Lahore. Inspired with the Swadeshi Movement several Swadeshi banks were established but few were survived to the present. Those were Bank of India, Corporation Bank, Indian Bank, Bank of Baroda, Canara Bank and Central Bank of India.\(^{57}\)

**Banks Failed During the period of First World War**

The period of First World War was unstable and number of banks were collapsed due to the Indian economy gaining indirect boost due to war-related economic activities.

Indian Companies Act was passed during 1913. This act is important because it is the first legislation related to banks. Though Indian Companies act contained some sections related to joint sector banks, it is inadequate to control banking activities. As a result of that Swadeshi movement was ended up in a bank failure during 1913-18. Majority of the banks that failed were small and weak. The failure of banks during this period lost the public faith in Indian banks and gave jolt to development of banking in India.

There was a brief interval in bank failures from 1918-21. The growth in economy after World War I gave one more momentum to the formation of new banks. A number of banks were opened; some of them were particularly for financing to industries. But from 1922, the bank failures took momentum due to depression in the economy. An act of amalgamation of three presidency banks\(^\_1920\) was enacted. Three presidency banks namely Bank of Bombay, Bank of Madras & Bank of Madras were amalgamated into Imperial Bank of India in 192. The Imperial Bank was effectively performing the functions of Central Bank of the country till the establishment of RBI in 1935.

\(^{57}\) Source: http://en.wikipedia.org/wiki/Banking_in_India#History
2.1.3(B) PHASE-II (1935-1968)

Pre-nationalization phase of Indian Banking

Phase II elaborates the developments of Indian Banking from 1935 to 1968. It describes after independence how government adopted policy resolution which resulted into greater involvement of the state in different segments of the economy including banking and finance. On the recommendation of Hilton Young Currency commission in 1928 for the creation of a separate bank, Reserve Bank of India was established in 1935 for the performance central banking functions. The important events those were taken place during this phase are as under:

i) In 1935, Reserve Bank of India was established:

To counter the economic troubles after the First World War The Reserve Bank of India, was established on 1st April, 1935 in accordance with the provisions of the Reserve Bank of India Act, 1934. It was established according to the guidelines laid down by Dr. Ambedkar. RBI was conceptualized as per the guidelines, working style and outlook presented by Ambedkar in his book “The Problem of the Rupee – It's origin and it’s solution” and also in front of the Hilton Young Commission.

ii) In 1949: Banking Regulation Act was enacted

The partition of India in 1947 badly affected the financial system of Punjab and West Bengal. The independence of India started the government intervention in the Indian banking. Government has adopted the Industrial Policy in 1948 by predicting a mixed economy. In 1949, the Banking Regulation Act was enacted which empowered the Reserve Bank of India (RBI) "to regulate, control, and inspect the banks in India. It also provided that no new bank or branch of an existing bank could be opened without a license from the RBI, and no two banks could have common directors. To streamline the functioning and activities of commercial banks, the Government of India came up with The Banking Companies Act, 1949 which was later changed to Banking Regulation Act 1949 as per amending Act of 1965 (Act No. 23 of 1965) and Reserve Bank of India

60 RBI Publications, Source: http://www.rbi.org.in
was given extensive powers for the supervision of Banking in India as the Central Banking Authority

iii) In 1955, State Bank of India was nationalized 61

In 1955, it nationalized Imperial Bank of India with extensive banking facilities on a large scale specially in rural and semi-urban areas. It formed State Bank of India to act as the principal agent of RBI and to handle banking transactions of the Union and State Govt. all over the country62

iv) In1959, Seven Subsidiaries of State Bank of India were nationalized63

After nationalization of State Bank of India ,seven banks forming Subsidiary of State Bank of India were nationalized in 1959 namely 1) State Bank of Bikaner & Jaipur, 2) State Bank of Hyderabad , 3) State Bank of Indore*( merged with SBI on 15 July 2010),4) State Bank of Mysore , 5) State Bank of Patiala , 6) State Bank of Saurahstra** ( merged with SBI on 13 September 2008) and 7) State Bank of Travancore

v) In 1961, Deposit Insurance Corporation was established64:

Deposit insurance, was established in India in 1962.Due to the Banking crises and bank failures in the 19th century as well as the early 20th Century (1913-14) the need for depositor protection in India was significantly felt. The banking crisis in Bengal between 1946 and 1948, pave the way for the revision of the issue of deposit insurance..

vi) In 1964,

The Industrial Development Bank of India (IDBI) was set up65:

The Industrial Development Bank of India (IDBI) was established on 1 July 1964 under an Act of Parliament as a wholly owned subsidiary of the Reserve Bank of India to serve as an Apex institution for Term finance for industries in India

61 RBI Publications,Source:http://www.rbi.org.in
62 ibid
63 ibid
64 ibid
2.1.3(C) PHASE-III (1969-1979)
Post-nationalization phase of Indian Banking

Phase III is known as “The Post Nationalization Phase of Indian Banking” and describes the progress of Indian Banking from 1969 to 1979. It throws the light on nationalisation of banks and explains how the reforms in banking sector have lead to the expansion of commercial banks and their branches all over the country. Bank credit was made instrumental for economic development of the country by way of spreading the banking habit among the people under the scheme of ‘Social Control’ of banks introduced in 1968.

i) In the year 1969, Major 14 Banks were nationalized.
By the 1960s, the Indian banking industry is instrumental in the development of Indian economy. Indira Gandhi, the then Prime Minister of India, expressed the intention of the Government of India in the annual conference of the All India Congress Meeting in a paper entitled “Stray thoughts on Bank Nationalization.” The meeting received the paper with enthusiasm.66
The following 14 largest commercial banks were nationalized with effect from the midnight of July 19, 1969 by issuance of the ordinance by Government of India.
The nationalization of 14 Commercial banks in July, 1969 was the height of Social control of banks. India switched over to mass banking from class banking trying to realize the social

ii) In 1971, Credit Guarantee Corporation (CGC) established.67
The Reserve Bank promoted a public limited company on January 14, 1971, named as Credit Guarantee Corporation of India Ltd. (CGCI). The credit guarantee schemes

67 Source: http://dicgc.org.in
introduced by the CGCI Ltd. with an intention to encourage the commercial banks to provide the credit needs to the neglected sectors of the society.

iii) In 1974, “Tandon Committee” was constituted for formulation of guidelines for the banks for follow-up of credit effectively.68

In 1974, a study group under the chairmanship of Mr. P. L. Tandon was constituted. Its main recommendations related to norms for inventory and receivables, the approach to lending, style of credit, follow ups & information system. With acceptance of major recommendations by Reserve Bank of India, a new era of lending began in India.

a) Talwar Committee was appointed to look into the Customer Service in banks69.

In 1975, the RBI has appointed the ‘Talwar Committee on Consumer Services in Banks’ and it recommended that, computerization of some functions to avoid delays in customer service in Indian banks.

b) Regional Rural Banks for Providing banking facilities to rural and semi-urban areas established 70.

Regional Rural Banks were established under the provisions of an ordinance passed on the 26th September 1975 and the RRB Act, 1976 for providing sufficient banking and credit facility for agriculture and other rural sectors. Likewise it was aimed to provide banking facilities to rural and semi-urban areas, to carry out government operations.

vi) In 1979:

a) Chore Committee was appointed to review the cash credit system

was established for rational management of funds by commercial banks.

b) Integrated Rural Development Programme (IRD P) was launched.

IRDP was launched in 1979 with twin objectives of raising family income of identified group of below poverty line and create sustained employment in rural areas. Initially the programme covered 2300 blocks excluding Districts covered under Small Farmer Development Agency and Marginal Farmer Development Agency

---

70 Source: http://en.wikipedia.org/wiki/Regional_Rural_Bank
2.1.3(D) PHASE-IV (1980-1990)
Preparatory phase of E-Banking in India

Phase-IV elaborates the development of Indian Banking since 1980 to 1990. This phase of banking is termed as “The Preparatory Phase of E-Banking in India”. Indian Banking Sector Reform further gain momentum by way of Second phase of nationalization of six more banks carried out in 1980. The reason for the nationalization was to bring credit delivery under the government control. Due to nationalization of six more banks, around 91% of the banking business of India came under the control of Government of India, The use of computers had led to introduction of online banking in India.

The RBI since 1984 formed various Committees on Mechanization & Computerization in the Banking Industry. This phase witnessed as the preparatory phase of electronic banking. During this decade RBI & Government prepared the platform to takeoff the electronic banking in India to the soaring heights. Followings measures have been initiated by RBI & Government of India in this regards:

i) In 1980, Nationalizations of Six Banks with Deposits over 200 Crore.\(^{71}\) in order to provide government more power and command over credit delivery, six more commercial banks in India were nationalized i.e. 1) Andhra Bank, 2) New Bank of India,, 3) Oriental Bank of Commerce, 4) Corporation Bank, 5) Punjab & Sind Bank and 6) Vijaya Bank

ii) Working Group” to consider feasibility of introducing MICR/OCR Technology for Cheque Processing established\(^ {72}\)

Under the Chairman-ship of Dr.Y.B.Damle, Adviser of Management Services Department, Reserve Bank of India a Working Group to consider feasibility of introducing MICR/OCR Technology for Cheque Processing established in 1982. The working group has recommended the introduction of 'item processing' (sorting and listing of cheques with the help of computers) in three phases.

In the first phase at the four metropolitan cities viz. Mumbai, New Delhi, Chennai and

---

\(^{71}\) Sopurce:http://www.rbi.org.in/rdoc.in/Publications/PDFs/4459.pdf

\(^{72}\) ibid
Calcutta, with the help of MICR technology. In the second phase all state capitals and important commercial centers. In the third & final phase national clearing to be introduced by dividing the country into four Regional Grids with headquarters at Mumbai, New Delhi, Chennai and Calcutta.

iii) In1983, Committee on Computerization and Mechanization was established\(^\text{73}\) to make recommendations for bank computerization and mechanization in the Banking Industry

In 1983 the RBI has appointed another committee under the chairmanship of Dr. C. Rangarajan, Deputy Governor, Reserve Bank of India to make recommendations for bank computerization and mechanization in the Banking Industry and suggest special plan for its implementation.

Dr. C. Rangarajan recommended that computerization and installation of Advanced Ledger Posting Machines (ALPM) at branch, regional and head offices of banks will bring around a new era in banking. Committee on mechanization of banks recommended that banks should set up service branches at centers where they have more than 10 branches. The service branch so set up would exclusively be devoted to clearing operations of the bank at that particular centre. Banks to be in readiness for the introduction of MICR Clearing at the four metropolitan cities by assessing their requirements for encoders, adopting standardized cheque forms and reorganizing work procedures where necessary, and training staff down to the branch level.

iv) In 1987, HSBC introduced Automated Teller Machine Concept (ATM) in India\(^\text{74}\) and India got its 1\(^{st}\) Automated Teller Machine (ATM) when HSBC Bank introduces ATM concept in India in 1987 and installed its ATM in India. Now-a-days, it is the common scene in most of the cities and town in India that Automated Teller Machines are installed at every nook & corner, at every nook and corner in most of the towns & cities. Likewise First Credit card was introduced by Andhra Bank\(^\text{75}\) and has lead the way of credit cards in India. The first credit cards were introduced in 1987 by Andhra Bank.

\(^{73}\) RBI Publications, Source: http://www.rbi.org.in

\(^{74}\) http://articles.timesofindia.indiatimes.com/2006-08-12/open-space/27790559_1_atm-india-credit

\(^{75}\) http://wiki.answers.com/Q/Which_was_the_first_Indian_Bank_to_introduce_credit_card
V) Under the Chairman-ship of Shri T.N.Iyer, Executive Director of Reserve Bank of India, a committees on Communication Network for Banks and SWIFT Implementation was established (1987). The committee recommended for setting up of packet switching network called 'BANKNET' to be jointly owned by the Reserve Bank and the public sector banks. The committee further recommended that India should join the SWIFT (Society for Worldwide Interbank Financial Telecommunication) Network for the transmission and reception of international financial messages and BANKNET should strive to emulate SWIFT in matters of data security, encryption, and authentication and SWIFT message standards which are internationally accepted should be adopted by BANKNET

vi) Indian Bank installed country's first ATM in 1988 and also the first drive-in ATM for the same bank.

vii) Committee on Computerisation in Banks established

In 1988, the RBI set up the Committee on Computerisation in Banks headed by Dr. C.R. Rangarajan, Deputy Governor of Reserve Bank of India. Committee recommended that computerisation of the settlement operations in the clearing houses managed by RBI at Bhubaneswar, Guwahati, Jaipur, Patna and Thiruvananthapuram. Operationalisation of MICR technology and the National Clearing of inter-city cheques at the four metropolitan cities i.e at Chennai, Delhi, Kolkata & Mumbai. Introduction of one-way collection of cheques drawn on the four metros received from Ahmedabad, Bangalore, Nagpur and Hyderabad. Framing of uniform rules and regulations of clearing houses, branch level computerisation and the establishment of connectivity between branches. Improvements in customer service - introduction of on-line banking. Setting up a network of Automated Teller Machines (ATMs) in Mumbai. Introduction of a single 'All Bank' credit card to reduce the load on cash and cheque transactions.

viii) In 1989, Kisan Credit Card introduced. Kisan Credit Card is a credit card was launched on August 5, 1998 designed offering the reasonable credit to Indian farmers. It was the joint venture of Government of India, RBI and NABARD.
2.1.3(E) PHASE-V(1991to2000)

Emergent phase of E-Banking in India

This phase is recognized as an emergent phase of e-banking in India and introduced various reforms and lots of products and facilities for implementation of e-banking. The Indian Financial System consisted of titanic network of branches of banks and financial institutions and plenty of financial products. The Indian financial system registered its presence among the people since nationalization of major banks and establishment of various financial institutions. The expansion of banking and other financial services to huge section of customers recognized as a noteworthy achievement in nineties. Other prominent measure were taken during this emergent phase of e-banking including enactment of ITAct 2000 enlisted as under:

i) In the year 1991 The Government of India appointed a Narasimham Committee called 'The Committee on Financed System' under the Chairmanship of Sri M., ex-Governor of Reserve Bank of India which made recommendations in November 1991. The committee recommended that banking structure of the Indian banking should be with 3 to 4 large banks (including SBI) at top and at bottom rural banks engaged in agricultural activities80.

ii) In1992: Income recognition and asset classification norms introduced

Provisioning and Capital adequacy standards specified. Indian Banks required to fulfill these norms by 1994 and 199681. Similarly SEBI was established in the year 1988 and given statutory powers on 12 April 1992 through the SEBI Act, 1992. SEBI has also to supervises functions of stock exchanges as well as act as an intermediaries.

---

80 RBI publications - crisis and reforms 1991-2000
80 ibid
81 ibid
iii) In 1993, New Bank of India merged with Punjab National Bank (PNB), and guidelines for establishment of 10 Private Sector Banks issued\(^{82}\). In the first round, RBI issued licenses to 10 private sector banks in 1993-94, shortly after the nation embraced economic liberalization under the P.V. Narasimha Rao government.  


iv) In 1994, Saraf Committee on Technology Issues was set up \(^{83}\)

A committee was set up in 1994 under the chairmanship of Shri W.S.Saraf, Executive Director, Reserve Bank of India on Technology Issues relating to Payments System, Cheque Clearing and Securities Settlement in the Banking Industry. Committee has submitted its Recommendations for establishment of an Electronic Funds Transfer (EFT) system, with the BANKNET communications network as its carrier.

v) In 1995:

a) National Securities Clearing Corporation Ltd. (NS CCL) was set up\(^{84}\)

NCCCL was incorporated in August 1995. It is wholly owned subsidiary of NSE and It was set up to bring and sustain confidence in clearing. It commenced clearing operations in April 1996.

b) Electronic Clearing Service was introduced by RBI\(^{85}\)

The Electronic Clearing Service (ECS) introduced by the RBI in 1995. ECS has two variants- ECS debit clearing and ECS credit clearing service. ECS credit clearing is used for transactions like payment of salary, dividend, pension, interest etc. ECS debit

---

\(^{82}\) Ibid  
\(^{83}\) RBI Publication-crisis and reforms 1991-2000  
\(^{84}\) RBI Publications, Source: http://www.rbi.org.in  
\(^{85}\) http://www.dnb.co.in/bfsisectorinindia/BankC6.asp
is used by utility service providers for collection of electricity bills, telephone bills and other charges and also by banks for collections of principal and interest repayments.

c) Shere Committee for proposing Legislation On Electronic Funds Transfer and other Electronic Payments established

A committee was set up in 1995 under the Chairpersonship of Smt. K. S. Shere, Principal Legal Advisor, Reserve Bank of India for proposing Legislation On Electronic Funds Transfer and other Electronic Payments. Committee recommended that EFT (Electronic Funds Transfer) system could be introduced immediately by framing regulations under Section 58 of the RBI Act.

vi) In 1996, the Institute of Development and Research in Banking Technology (IDR BT) established.

The first phase of reforms in the Indian Financial Sector felt the dire need for an High Level Institute, for implementing Banking Technology in the Indian Banking and Financial Sector. IDBRT was established in 1996 by RBI. IDBRT is having its headquarter at Hyderabad. The main objective of setting up IDBRT by RBI for providing the operational service support in Information Technology to Banks and Financial Institutions.

vii) In 1997: “Khan Working Group” instituted

The group was set up by the RBI in December 1997 to review the role and structure of the developing financial institutions and commercial banks in the emerging environment, recommended several interim measures towards achieving coordination and harmonisation of the lending policies of banks and financial institutions before they move towards universal banking.


Electronic Commerce Support Act, 1998 enacted. suitable amendments were made to the following acts namely 1) Amendment to the Indian Evidence Act, 1872, 2)

b) Narasimham Committee-Il constituted (II\textsuperscript{nd} Generation Reforms)\textsuperscript{90}
Under the chairmanship' of Mr. Narasimham, Government appointed a second high-level Committee on Banking Sector Reforms to review the progress of banking sector.

c) Vasudevan Committee for Technology Up-gradation in the Banking Sector formulated\textsuperscript{91}
The committee, headed by RBI Executive Director, A. Vasudevan was constituted in September 1998.

Committee has given recommendations on 1) Communication infrastructure and use of INFINET, 2) Standardisation and security, 3) Outsourcing of Technology and service, 4) Computerisation of Govt. Transaction, 5) Set up date warehousing, mining and MIS by January 1, 2001 and 6) An amendment to the Reserve Bank of India Act, 1934 to enable the central bank regulate and supervise payment and settlement system

ix) In 1999, RBI issued guidelines for the issuance of Debit and Smart Cards\textsuperscript{92}
The banks can issue smart/on-line debit cards to select customers with good financial standing even if they have maintained the accounts with the banks for less than six months subject to their ensuring the implementation of 'Know Your Customer' concept

x) In 2000 : a) Credit Information Bureau (India) Limited (CIBIL) founded
Credit Information Company (CIC) founded in August 2000. CIBIL collects and maintains records of borrowers’ payments records pertaining to loans and credit cards.

b) Enactment of Information Technology Act 2000
Information technology is one of the important law relating to Indian cyber laws. It had passed in Indian parliament in 2000. This act is helpful to promote business with the help of internet. It also set of rules and regulations which apply on any electronic business transaction. Due to increasing crime in cyber space, Govt. of India understood the problems of internet user and for safeguarding the interest of internet users, this act was made.

\textsuperscript{90} RBI Publications, Source: http://www.rbi.org.in
\textsuperscript{91} ibid
\textsuperscript{92} ibid
2.1.3(F) PHASE-VI (2001-2008)
Transitional phase of E-Banking in India
The Government of India took a series of measures to create requisite institutional infrastructure of financial market after enactment of ITA2000 which includes the following:

i) In 2001:
   a) Core Banking Solutions (CBS) implemented
      Syndicate Bank was the first bank among public sector banks who introduced CBS in the year 2001. Core Banking Solution (CBS) is the connectivity between the recognized branches and all the ATMs of the bank connected to a powerful Central Computer System at the Data Centre. This connectivity is established through leased telephone lines. The data of recognised branches connected with the Central Computer System would be uploaded on the Central Computer System in the Data Centre. This method allowed the customer to perform banking transactions from any of the branches connected with the Net Work during the working hours. Any Time Any Where Banking became possible by using ATM & Internet. Here the concept of Branch Banking is closed down and Bank Banking established. The CBS system enables banks to curtail their transaction cost by using the technology.
   b) RBI issued guidelines on Universal Banking
      R.H. Khan Committee had recommended the concept of Universal Banking. Universal Banking means allowing financial institutions (FIs) and banks to undertake all kinds of activity of banking or development financing or activity associated with that, subject to compliance of statutory and requirements prescribed by RBI, Government and related legal Acts.
   c) Clearing Corporation of India Ltd. (CCIL) was incorporated
      On 30th April, 2001 The Clearing Corporation of India Ltd. (CCIL) was incorporated for providing the safe institutional arrangement for the clearing and settlement of trades in the Government Securities, Forex (FX) Monetary and Debt markets, CCL has been set up. CCIL commenced its operations on 15th February, 2002

93 RBI Publications, Source: http://www.rbi.org.in
94 Toor, N.S., Handbook of Banking Information, Skylark Publications, 28th edition 2009 p 1.16-1.17
95 RBI Publications, Source: http://www.rbi.org.in
ii) In 2002, Anti Money Laundering Act, 2002 enacted by Indian Parliament

Anti Money Laundering Act, 2002 was passed by Indian Parliament in the year 2002. The Act was made effective from 1st July, 2005. The Act specifically described the legislative duties of banking companies, financial institutions and intermediaries. The intention of this law was to fulfill with the duties specified in this act to support the law enforcement agencies. The act is useful to identify proceeds originated from grave crimes. It would prevent money laundering &terrorist financing and recycling of illegally money earned by the miscreants.

iii) In 2004,

a) RBI set up the Khan Commission in 2004 to look into financial inclusion

The recommendations of “Khan Commission” were incorporated into the mid-term review of the monetary policy of RBI(2005–06). In the report RBI urged the banks with a vision to achieve greater financial inclusion to make available a "no-frills" account which is the basic need of financial inclusion. In India, financial inclusion first featured in 2005, when it was introduced by K.C. Chakraborthy, the chairman of Indian Bank. “

b) The Real Time Gross Settlement (Membership) Regulations, 2004 was framed

The short form 'RTGS' stands for Real Time Gross Settlement, which can be defined as the continuous (real-time) settlement of funds transfers individually on an order by order basis (without netting). The RTGS system is primarily meant for large value transactions. The minimum amount to be remitted through RTGS is ` 2 lakh. There is no upper ceiling for RTGS transactions. The RTGS service window for customer's transactions is available from 9.00 hours to 16.30 hours on week days and from 9.00 hours to 13.30 hours on Saturdays for settlement at the RBI end.

---

iv) In 2005,

a) “No Frills Account” was introduced in November 2005

No Frill Account was introduced in 2005 which is now called as “Basic Savings Bank Deposit Account” where there is no need to provide minimum balance, by Banks and Co-operative Banks. The Account will have the facility of ATM-cum-Debit Card without any charges. There is no restriction for number of cash credits to the account. The account-holder also has the overdraft facility of `500/-.

c) RBI National Electronic Fund Transfer (NEFT) System was established

RBI has introduced an electronic funds transfer system called "The RBI National Electronic Funds Transfer System" (herein after may be referred to as "NEFT System" or "System") in November 2005 The objects of the NEFT System are to establish an Electronic Funds Transfer System to facilitate an efficient, secure, economical, reliable and expeditious system of funds transfer and clearing in the banking sector throughout India, and to relieve the stress on the existing paper based funds transfer and clearing system. A lot of transactions are settled in one go in each batches

v) In 2006, Branchless banking through Business Correspondent model was introduced

With the objective of ensuring greater financial inclusion and increasing the outreach of the banking sector, it has been decided in public interest to enable banks to use the services of Non-Governmental Organisations/ Self Help Groups (NGOs/ SHGs), Micro Finance Institutions (MFIs) and other Civil Society Organisations (CSOs) as intermediaries in providing financial and banking services through the use of Business


The PSS Act, 2007 received the assent of the President on 20th December 2007 and it came into force with effect from 12th August 2008. The PSS Act, 2007 provides for the regulation and supervision of payment systems in India and designates the Reserve Bank of India (Reserve Bank) as the authority for that purpose and all related matters. The Act also provides the legal basis for “netting” and “settlement finality”. This is of

100 Source: http://rbidocs.rbi.org.in/rdocs/content/pdfs/67253.pdf
great importance, as in India, other than the Real Time Gross Settlement (RTGS) system all other payment systems function on a net settlement basis.

vii) In 2008,

a) National Payments Corporation of India (NPCI) was incorporated \(^{102}\)
National Payments Corporation of India (NPCI) was incorporated in December 2008 and the Certificate of Commencement of Business was issued in April 2009. It has been incorporated as a Section 25 company under Companies Act and is aimed to operate for the benefit of all the member banks and their customers. Presently, there are ten core promoter banks (State Bank of India, Punjab National Bank, Canara Bank, Bank of Baroda, Union bank of India, Bank of India, ICICI Bank, HDFC Bank, Citibank and HSBC).

b) The National Electronic Clearing Services (NECS) system was implemented\(^{103}\).
Shri V. Leelaadhar, Deputy Governor, Reserve Bank of India inaugurated the National Electronic Clearing Service (NECS) at a function at the Reserve Bank's National Clearing Centre (NCC), Mumbai in September 2008. The service was implemented with an aim to centralize the Electronic Clearing Service (ECS) operation and bring in uniformity and efficiency to the system.

c) Mobile Banking Transactions in India – RBI issued Guidelines for Banks\(^{104}\)
RBI issued Operative Guidelines for Banks on Mobile Banking Transactions in India on September 19, 2008. Mobile phones as a delivery channel for extending banking services have off-late been attaining greater significance. The rapid growth in users and wider coverage of mobile phone networks have made this channel an important platform for extending banking services to customer.

d) Information Technology (Amended) Act, 2008 enacted\(^{105}\)
The Information Technology Act, 2000 was amended by Information Technology Amendment Bill 2006. The Information Technology (Amendment) Bill, 2008 (Bill No. 96-F of 2008) was passed by the both houses of parliament on December, 2008 and

\(^{102}\) http://www.npci.org.in/aboutus.aspx
\(^{104}\) http://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/87064.pdf
received the accent of the president on 5th February, 2009. However, after the wait of almost more than 8 months, the Information Technology (Amendment) Act, 2008 (ITAA, 2008) has been notified with effect from 27/10/2009 and is now become operational.

2.1.3(G) PHASE-VII (2009-2013)

Matured Phase of E-Banking in India

After enactment of ITAA-2008, Indian Banking Industry entered into the matured phase E-Banking.

i) In 2009,

a) Branch Licensing Policy 2009-RBI

To address the issue of uneven spread of Bank Branches, since December 2009, domestic scheduled commercial banks are permitted to freely open branches in Tier 3 to Tier 6 centers with population of less than 50,000 under general permission, subject to reporting. In the North Eastern States and Sikkim, domestic scheduled commercial banks can now open branches in rural, semi urban and urban centers without the need to take permission from RBI in each case, subject to reporting. Reserve Bank advised commercial banks that while preparing their Annual Branch Expansion Plan (ABEP), they should allocate at least 25 per cent of the total number of branches proposed to be opened during the year in unbanked rural centers. For this purpose, the centers are classified based on population, viz. Tier-I: Population of 1,00,000 and above, Tier-II : Population of 50,000 to 99,999 Tier-III: Population of 20,000 to 49,999. Tier-IV: Population of 10,000 to 19,999 Tier-V: Population of 5,000 to 9,999 and Tier-VI: Population of less than 5,000.

(Source: RBI Cir. BL. BC/65/22.01.001/2009-10 dt. 1st Dec. 2009)

b) Aadhaar -The Unique Identification Authority of India (UID) was launched

The Unique Identification Authority of India (UIDAI) was established in January 2009 and is part of the Planning Commission of India. UIDAI aims to provide a unique 12 digit ID number to all residents in India on a voluntary basis. The number will be known as Aadhaar.

107 http://cis-india.org/internet-governance/blog/uid-and-npr-a-background-note
ii) In 2010, the Base Rate system was formulated\textsuperscript{108}

The Base Rate system has replaced the BPLR system with effect from July 1, 2010. Base Rate shall include all those elements of the lending rates that are common across all categories of borrowers. Banks may choose any benchmark to arrive at the Base Rate for a specific tenor that may be disclosed transparently.

iii) In 2011,

a) Swabhiman – Our Account Our Pride was launched\textsuperscript{109}

Swabhiman Campaign is the campaign started by the Ministry of Finance, Government of India and the Indian Banks Association (IBA) (an association of most of the Indian banks) to bring banking within the reach of the masses of the Indian population. The aim of the government is to bring a bank within the reach of every village with a population of over 2000 by the end of March, 2012. The bank in the village will facilitate the opening of an account by a villager. It will provide a need-based credit to the villagers. Remittance facilities to transfer funds from one place to another will also be the part of the banking services to

b) Electronic Benefit Transfer (EBT) and its convergence with Financial Inclusion Plan (FIP) Launched\textsuperscript{110}.

Vide circular RBI/2011-12/153RPCD.CO.BC.FID.No. 16/12.01.019/2011-12 dated August 12, 2011 RBI issued operational guidelines for implementation of Electronic Benefit Transfer and its convergence with Financial Inclusion Plan. Electronic Benefit Transfer (EBT) implementation will enable the beneficiaries to get the social security benefits directly credited to their accounts and at the same time it will relieve the Government functionaries of the cost and time involved in manually administering the high volume and low value payment.

iv) In 2012

a) RBI releases guidelines on White Label Automated Teller Machines (WLAs)\textsuperscript{111}

The Reserve Bank of India, on its website, the final guidelines on "White Label Automated Teller Machines (WLAs) in India". White Label ATMs are ATMs set up,

\textsuperscript{108} ww.allbankingsolutions.com/Banking-Tutor/Base-Rate-vs-BPLR-Benchmark-Prime-Lending-Rate.shtml
\textsuperscript{109} By Gitchandra Oinam, Essay as title “Swabhiman -Our future our pride” published on http://epao.net/
\textsuperscript{110} http://www.rbi.org.in/scripts/NotificationUser.aspx?id=6673&Mode=0
\textsuperscript{111} http://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=26693
owned and operated by non-bank entities incorporated in India under the Companies Act, 1956. Till now, only banks were permitted to set up Automated Teller Machines (ATMs) as extended delivery channels. In order to deep penetration on ATMs in unbanked and under banked areas, RBI has permitted ‘White Label ATMs’ in the country to supplement the existing ATMs.

b) Cheque Truncation System-RBI Guidelines:\(^{112}\):
The Cheque Truncation System (CTS) is image based clearing process.. Under CTS physical movements of cheques from the branch to clearing house and vice-versa prevented. Instead the electronic image of the cheque would be sent to the clearing house. It enables the realization of cheques on the same day and provide a more cost effective mode of settlement than manual and MICR clearing. The CTS has been launched in February 2008 on pilot basis in the NCR of New Delhi.

v) In 2013, Master circular on Mobile Banking Transactions in India -RBI\(^{113}\):
RBI has issued Operative Guidelines for Banks vide circular no RBI/2013-14/116 DPSS.CO.PD. Mobile Banking. No./02.23.001/2013-14 dated July 1, 2013. The Master Circular has been updated by incorporating all the instructions/ guidelines issued on Mobile Banking up to June 30, 2013. 

**Previous Guidelines consolidated:** The Master Circular compiles the instructions contained in the circulars issued on Mobile Banking as under:
Almost all the banks in India have adopted Information Technology to render banking services to their customers by using the IT tools & techniques to fulfill the needs of the customers. Now days, due to adoption of information technology, banking is also shifted from paper based banking to paperless banking and anytime anywhere banking is possible.

*****

\(^{112}\) http://rbi.org.in/scripts/FAQView.aspx?id=63
\(^{113}\) http://www.google.co.in/#q=RBI%2F201314%2F116+DPSS.CO.PD.+Mobile+Banking.
2.2 MEANING & CONCEPT OF E-BANKING

Banking industry has gone through major amendments in recent past. These amendments have been taken place due to deregulation policy of government, to make open the regional markets to the global entities due to the adoption of digital net work by the customers. The development and growth of internet banking is definitely one of the most powerful drivers in the restructuring of banking services. The previous dependence on large networks of branch offices has been replaced by digital services.

All over the world there were various sweeping changes in the economic and banking atmosphere in the last decade of the 21st century all over the world. Due to the overall changes in the economic and financial sector since early 1990s, simultaneously introduced working filed of banks in India undergone a swift change. Due to the process of deregulation and reforms in the Indian banking system it impact directly resulted in the creation of an efficient and competitive banking system. New avenues were open up due to deregulations for banks to increase their revenues by expanding into universal banking, investment banking, bank assurance, mortgage financing, depository services, securitization, personal banking etc.

Liberalization has opened the new avenues to new banker and put the greater competition among banks. All over the world, the ICT (information and communication technology) drastically added handful growth and profit of financial institutions. Technology is the instrument to make available banking services to customers in a efficient manner. As the latest technology was adopted by the banks globally, Indian banking has also adopted the latest technology but very late for stay and survive in the global competition..

2.2.1 TRANSFORMATION OF INDIAN BANKING SECTOR

There are various elements which have an impact on the Indian banking sector for adoption of technology.\textsuperscript{115}

1) Government of India introduced the economic reforms in 1991 which open the doors for new opportunities for banks all over the world.

2) As a part of strategy of the government Indian banking was made available for private sector banks. Private sector banks utilized the opportunity and they boost up the technology and created an environment to use it for back office as well as and front-office operations. With the result of such competitions among the banks, entire banking system became more vibrant and more efficient. The banks and customer both became techno savvy.

3) In the last few years, with the development of telecom sector, communication infrastructure, the entire cities and places of India got connected with each other. This contributes to reduce the cost of the banks in India. During the same period banks adopted the CBS technology for connecting the branches in the country by offering banking services anywhere and anytime.

4) Indian software industry has also contributed the Indian banking sector. The customer service provided by the Banks to their customers, software companies came forward to help banks by providing web based portals, wide area network (WAN), local area network, internet, etc. at affordable prices and at the high time.

5) Fifthly, as per the directives of RBI to adopt the changes in order to improve the operational efficiencies, security measures, risk reduction and quality up-gradation maximum banks in the country have adopted the new technology.

After liberalization RBI has designed several changes in the structure of banking sector and made compulsory several guidelines on electronic banking, fund transfer, core banking solution, payment system, clearing services, and internet banking. So, it becomes obligatory for the banks to adapt broad changes in technology. Indian Banking Association (IBA) has extended its helping hand to banks in this regard\textsuperscript{116}.

\textsuperscript{115} International Journal of Management (IJM), Volume 3, Issue 3, September- December (2012)

\textsuperscript{116} Ibid
For the past three decades, the banking system of India has been hassle-free and able to meet new challenges posed by technology as well as external and internal factors.

Source: Included in the Second Schedule of Reserve Bank of India Act, 1934
India’s banking system has several outstanding achievements to its credit includes both Public Sector Banks, and the Private Sector Banks. In Public Sector Banks, the government must retain a 51% stake.

Old Private sector banks are those banks which were not nationalized at the time of bank nationalization that took place during 1969 and 1980. Most of the old private-sector banks are closely held by certain communities and their operations are mostly restricted to the areas in and around their place of origin. e.g Federal Bank, Dhanalaxmi Bank, ING Vyasya Bank.

New private sector banks include those that were established in the past twenty years such as Yes Bank, Axis bank and existing institutions that were converted into commercial banks, such as the former development institution ICICI and specialized lenders such as HDFC.

Cooperative banks are small-sized units registered under the Co-operative Societies Act., that essentially lend to small borrowers and businesses. Eg. Punjab & Maharashtra Co-op. Bank Ltd., New India Co-op. Bank Ltd.

Regional Rural Banks are mainly focused on the agro sector. These banks are in every corner of the country and extend a helping hand in the growth of the country. Eg. National Bank for Agriculture and Rural Development (NABARD), Haryana State Cooperative Apex Bank Limited.

Also, under the recently passed The Banking Laws (Amendment) Bill 2011, the government is likely to give the new banking licenses by 31st March 2014.

**SCHEDULED BANKS**

A scheduled bank is a bank that is listed under the second schedule of the RBI Act, 1934. In order to be included under this schedule of the RBI Act, banks have to fulfill certain conditions such as having a paid up capital and reserves of at least 0.5 million and satisfying the Reserve Bank that its affairs are not being conducted in a manner prejudicial to the interests of its depositors.

Scheduled banks are further classified into commercial and cooperative banks.
**Schedule Commercial Banks**

Scheduled Commercial Banks (SCBs) account for a major proportion of the business of the scheduled banks. As at end-March, 2013, 169 SCBs were operational in India. SCBs in India are categorized into the five groups based on their ownership and/or their nature of operations. State Bank of India and its five associates (excluding State Bank of Saurashtra, which has been merged with the SBI with effect from August 13, 2008 and State Bank of Indore since merged with SBI w.e.f. 15 July 2010) are recognized as a separate category of SCBs, because of SBI Act, 1955 and SBI Subsidiary Banks Act, 1959. Nationalized banks (20) and SBI and associates (6), together form the public sector banks group and control around 70% of the total credit and deposits businesses in India. IDBI ltd. has been included in the nationalized banks group since December 2004. As at end-March 2013, there were 13 old and 7 new generation private sector banks operating in India. Foreign banks are present in the country either through complete branch/subsidiary route presence or through their representative offices. At end-March 2013, 41 foreign banks were operating in India with 331 branches. Regional Rural Banks (RRBs) were set up in September 1975 in order to develop the rural economy by providing banking services in such areas by combining the cooperative. RRBs have a unique structure, in the sense that their equity holding is jointly held by the central government, the concerned state government and the sponsor bank (in the ratio 50:15:35), which is responsible for assisting the RRB by providing financial, managerial and training aid and also subscribing to its share capital. Between 1975 and 1987, 196 RRBs were established. RRBs have grown in geographical coverage, reaching out to increasing number of rural clientele. At the end of June 2008, they covered 585 out of the 622 districts of the country. As a result of state wise amalgamation of RRBs sponsored by the same sponsor bank, the number of RRBs fell to 82 by end March 2013.
Scheduled Cooperative Banks

Scheduled cooperative banks in India can be broadly classified into urban credit cooperative institutions and rural cooperative credit institutions. Rural cooperative banks undertake long term as well as short term lending. Credit cooperatives in most states have a three tier structure (primary, district and state level)

NON-SCHEDULED BANKS

Non-scheduled banks also function in the Indian banking space, in the form of Local Area Banks (LAB). As at end-March 2013 there were only 4 LABs operating in India. Local area banks are banks that are set up under the scheme announced by the government of India in 1996, for the establishment of new private banks of a local nature; with jurisdiction over a maximum of three contiguous districts. LABs aid in the mobilisation of funds of rural and semi urban districts. Six LABs were originally licensed, but the license of one of them was cancelled due to irregularities in operations, and the other was amalgamated with Bank of Baroda in 2004 due to its weak financial position.

2.2.3 JOURNEY OF COMMERCIAL BANKING SINCE 1969 TO 2012

For the previous four decades India’s banking system has several excellent attainments to its credit. The government’s regulating policy for Indian bank since 1969 has came out with the nationalization of 14 major private banks of India This is one of the main reasons of India’s growth process.

Table 2.1- Expansion of Bank Branches since Nationalization (1969-2012)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Commercial Banks (incl. RRBs and LABs)</td>
<td>73</td>
<td>272</td>
<td>182</td>
<td>173</td>
</tr>
<tr>
<td>No. of Bank Branches of which Rural and semi-urban bank offices</td>
<td>8,262</td>
<td>60,570</td>
<td>74,563</td>
<td>1,01,261</td>
</tr>
<tr>
<td>Population per office</td>
<td>64,000</td>
<td>14,000</td>
<td>15,000</td>
<td>13,000</td>
</tr>
</tbody>
</table>

From the above table it reveals that No of Scheduled Commercial Banks were rise from 73 from 1969 to 173in 2012. Similarly rise of bank branches since 1969 was from 8262 branches to 60570 branches in 1991 while it rose to 74563 branches and finally rest on

118 RBI progress of commercial banks at a glance.
101261 branches. There is a substantial rise of rural and semi-urban branches from 1969 to 2012. The population per office is decreased due to expansion of the branches.

2.2.4 MAJOR BANKING SECTOR REFORMS SINCE 1991 119

The economic reforms initiated in 1991 also griped the banking system. Following are the major reforms aimed at improving efficiency, productivity and profitability of banks.

1) Granting functional autonomy to public sectors banks.
2) Liberalization of entry norms for banks. New banks licensed in private sector to inject competition in the system.10 in 1993 and 2 more in 2003. Another lot of new banks will be licensed by the end of March 2014
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.
8) FDI+FII up to 74% allowed in private sector banks
9) Listing of PSBs on stock exchanges and allowing them to access capital markets for augmenting their equity, subject to maintaining Government shareholding at a minimum of 51%. Private shareholders represented on the Board of PSBs.
10) Progressive reduction in statutory pre-emption (SLR and CRR) to improve the resource base of banks so as to expand credit available to private sector. SLR currently at 23% (38.5% in 1991) and CRR at 4% (15% in 1991).
11) Adoption of international best practices in banking regulation. Introduction of prudential norms on capital adequacy, IRAC (income recognition, asset classification, provisioning), exposure norms etc.
12) Phased liberalizations of branch licensing. Banks can now open branches in Tier 2 to Tier 6 centers without prior approval from the Reserve Bank.

119 http://r geared to.rbi.org.in/rdocs/Speec shee.pdfs/PDFs/FIBACSS130813.pdf
13) Deregulation of a complex structure of deposit and lending interest rates to strengthen competitive impulses, improve
14) Allocative efficiency and strengthen the transmission of monetary policy.
15) Base rate (floor rate for lending) introduced (July 2010). Prescription of an interest rate floor on savings deposit rate withdrawn (Oct. 2011).
16) Use of information technology to improve the efficiency and productivity, enhance the payment and settlement systems and deepen financial inclusion
17) Strengthening of Know Your Customer (KYC) and Anti-money Laundering (AML) norms; making banking less prone to financial abuse.
18) Improvements in the risk management culture of banks.

MARKET SHARE OF FINANCIAL ASSETS
Indian Financial System - Share by Asset Size - 2012\textsuperscript{120}

<table>
<thead>
<tr>
<th>Financial Segment</th>
<th>Market Share of Financial Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banks</td>
<td>63%</td>
</tr>
<tr>
<td>Insurance Companies</td>
<td>19%</td>
</tr>
<tr>
<td>Non-banking Financial Institutions</td>
<td>8%</td>
</tr>
<tr>
<td>Mutual Funds</td>
<td>6%</td>
</tr>
<tr>
<td>Provident and Pension Funds</td>
<td>4%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

MARKET SHARE OF BANKING ASSETS
Indian Banking System - Share by Asset Size Institution 2012\textsuperscript{121}

<table>
<thead>
<tr>
<th>Financial Segment</th>
<th>Market Share of Banking Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled Commercial Banks of Which</td>
<td>92.4%</td>
</tr>
<tr>
<td>a) Public Sector Banks</td>
<td>67.2%</td>
</tr>
<tr>
<td>b) Private Sector Banks</td>
<td>18.7%</td>
</tr>
<tr>
<td>c) Foreign Banks</td>
<td>2.7%</td>
</tr>
<tr>
<td>d) Rural &amp; Urban Co-operative Banks</td>
<td>3.4%</td>
</tr>
<tr>
<td>Local Area Banks</td>
<td>1.5%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

\textsuperscript{120} http://rbidocs.rbi.org.in/rdocs/Speeches/PDFs/FIBACS130813.pdf
\textsuperscript{121} Ibid
MARKET SHARE IN THE BANKING SPACE

Table 2.4 – No. Scheduled Commercial Banks their Branches & Market Share

<table>
<thead>
<tr>
<th>Type of Banks</th>
<th>Number of Banks</th>
<th>Number of Branches</th>
<th>Percentage Share of Number of Branches</th>
<th>Market Share of Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Sector</td>
<td>26</td>
<td>67,466</td>
<td>83.0</td>
<td>72.8</td>
</tr>
<tr>
<td>Private Sector</td>
<td>20</td>
<td>13,452</td>
<td>16.6</td>
<td>20.2</td>
</tr>
<tr>
<td>Foreign Banks</td>
<td>41</td>
<td>323</td>
<td>0.4</td>
<td>7.0</td>
</tr>
<tr>
<td>Total</td>
<td>87</td>
<td>81,241</td>
<td>100.0</td>
<td>100.0</td>
</tr>
</tbody>
</table>

While going through the above tables it reveals that:

- It reveals from the above that Indian Banking System is dominated by Commercial Banks.
- It reveals from the above that Public Sector Banks have more branch presence relative to their share of assets.
- Within the banking system, public sector banks (PSB) continue to dominate with 73% of market share of assets and 83% of branches.
- Rural and urban co-operatives banks have a relatively small share in the banking system. However, given their geographic and demographic outreach, they play a key role in providing access to financial services to low and middle income households in both rural and urban areas.
- Similarly, RRBs play a key role in promoting financial inclusion. The Government is pursuing branch expansion and capital infusion plans for the RRBs.

2.2.5 EXPANSION OF Banking SINCE NATIONALIZATION

Table 2.5 – Expansion of Banking Since 1969 to 2012

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Commercial Banks (including RRBs &amp; LABs)</td>
<td>73</td>
<td>272</td>
<td>182</td>
<td>173</td>
</tr>
<tr>
<td>No. of Bank Offices</td>
<td>8,262</td>
<td>60,570</td>
<td>74,563</td>
<td>1,01,261</td>
</tr>
<tr>
<td>of which Rural and semi-urban bank offices</td>
<td>5,172</td>
<td>46,550</td>
<td>47,179</td>
<td>62,061</td>
</tr>
<tr>
<td>Population per office</td>
<td>64,000</td>
<td>14,000</td>
<td>15,000</td>
<td>13,000</td>
</tr>
<tr>
<td>Per capita Deposit of Scheduled Commercial Banks (SCBs)</td>
<td>88</td>
<td>2,368</td>
<td>23,382</td>
<td>51,106</td>
</tr>
<tr>
<td>Per capita Credit of SCBs</td>
<td>68</td>
<td>1,434</td>
<td>1,7541</td>
<td>39,909</td>
</tr>
</tbody>
</table>

Effect of expansion of banking since nationalization are as under:

- Since nationalisation of 14 major commercial banks in 1969, followed by nationalisation of another 6 banks in 1980, Indian banking system has expanded rapidly.
- The number of bank offices increased from about 8,000 in 1969 to over 100,000 by 2012.
- The average population per branch office has sharply declined from 64,000 in 1969 to 13,000 today.
- Both per capita deposit and per capita credit have expanded about 600 times. Even accounting for inflation, this is significant expansion.

SCHEDULED COMMERCIAL BANKS IN INDIA AS ON 31/03/2012

[A] Following are the Public Sector Banks in India:

<table>
<thead>
<tr>
<th>SBI &amp; Associates</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. State Bank of India</td>
</tr>
<tr>
<td>2. State Bank of Hyderabad</td>
</tr>
<tr>
<td>3. State Bank of Patiala</td>
</tr>
<tr>
<td>4. State Bank of Bikaner and Jaipur</td>
</tr>
<tr>
<td>5. State Bank of Mysore</td>
</tr>
<tr>
<td>6. State Bank of Travancore</td>
</tr>
</tbody>
</table>

[B] Following are the Nationalised Banks in India

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

[B] Following are the Old Private Banks in India: 126

<table>
<thead>
<tr>
<th>No.</th>
<th>Bank Name</th>
<th>Bank Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Catholic Syrian Bank Ltd</td>
<td>City Union Bank Ltd.</td>
</tr>
<tr>
<td>2</td>
<td>Dhanlaxmi Bank Ltd</td>
<td>Federal Bank Ltd.</td>
</tr>
<tr>
<td>3</td>
<td>ING Vaisya Bank Ltd</td>
<td>Jammu &amp; Kashmir Bank Ltd</td>
</tr>
<tr>
<td>4</td>
<td>Karur Vysya Bank Ltd</td>
<td>Karnataka Bank Ltd.</td>
</tr>
<tr>
<td>5</td>
<td>Laxmi Vilas Bank Ltd</td>
<td>Nainital Bank Ltd</td>
</tr>
<tr>
<td>6</td>
<td>Ratnakar Bank Ltd</td>
<td>South Indian Bank Ltd</td>
</tr>
<tr>
<td>7</td>
<td>Tamilnad Mercantile Bank Ltd</td>
<td></td>
</tr>
</tbody>
</table>

[C] Following are the New Private Banks in India: 127

<table>
<thead>
<tr>
<th>No.</th>
<th>Bank Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Axis Bank Ltd</td>
</tr>
<tr>
<td>2</td>
<td>Development Credit Bank Ltd</td>
</tr>
<tr>
<td>3</td>
<td>HDFC Bank Ltd</td>
</tr>
<tr>
<td>4</td>
<td>ICICI Bank Lt</td>
</tr>
<tr>
<td>5</td>
<td>IndsInd Bank</td>
</tr>
<tr>
<td>6</td>
<td>Kotak Mahindra Bank Ltd.</td>
</tr>
<tr>
<td>7</td>
<td>Yes Bank Ltd</td>
</tr>
</tbody>
</table>

2.2.6 MEANING AND CONCEPT OF “E-BANKING” 128

E-bank is the electronic bank that provides the financial service for the individual client by means of Internet. E-banking means any user with a personal computer and a browser can get connected to his bank’s website to perform any of the virtual banking functions. In internet banking system the bank has a centralized database that is web-enabled. All the services that the bank has permitted on the internet are displayed in menu. Once the branch offices of bank are interconnected through terrestrial or satellite links, there would be no physical identity for any branch. It would be a borderless entity permitting anytime, anywhere and anyhow banking.

---

126 Source: http://www.gktoday.in/schedule-banks-of-india/
127 Source: http://www.gktoday.in/schedule-banks-of-india/
128 www.cab.org.in/.../8_e_banking_challenges_status_trends_Policy_Issues...
DEFINITION OF E-BANKING\textsuperscript{129}

E-banking is defined as the automated delivery of new & traditional banking products & services directly to customers through electronic, interactive communication channels. E-banking includes the systems that enable financial institution, customers, individuals & businesses to access accounts, transact business or obtain information on financial products & services through a network including the internet. In general E-banking is an umbrella term for the process by which a customer may perform banking transactions electronically without visiting a brick-and-mortar institution. The following terms all refer to one form or another of electronic banking: personal computer (PC) banking, Internet banking, virtual banking, online banking, home banking, remote electronic banking, and phone are banking. PC banking and Internet or online banking is the most frequently used designations. It should be noted, however, that the terms used to describe the various types of electronic banking are often used interchangeably.

PROGRESS OF E-BANKING\textsuperscript{130}

The progress of E-banking, after the liberalization and globalization processes began since 1991, influencing the financial sector, particularly on the banking sector. The advancement has thoroughly and perceptibility revamps the operational environment of the banking. The E-commerce drastic change is completely alter the way of client banking, banks are providing different services cash deposits to cash withdrawals through electronic means therefore we can say number of electronic transactions are increasing the world is going to be a cyber world where each and everyone would be connected through internet. The world is becoming a global market, characterized by economic interdependence. National boundaries have become less significant with the interlinked effect of technology, information flows and foreign investment mobility. In past thirty years, operational efficiency of banks increased now the time taken by the banks in different transaction has been reduced with this advancement competition is also increased .Banks are interested to acquire more and more customer to increase their revenue and using different tools of technology to increase the number of their

\textsuperscript{129} en.wikipedia.org/wiki/Online banking
\textsuperscript{130} Report on E-Banking Sourcewww.rbi.org.in › Publications
clients. E-banking is the service which the banks are providing now a day to provide
24X7 banking. In these days clients are not visiting the banks they are only using cyber
banking for each transactions by that way the banks are able to reduce their operating
cost also.

FUNCTIONS OF E-BANKING 131

a) Inquiry about the Information of Account :
The client inquires about the details of his own account information such as the card's / account’s balance and the detailed historical records of the account and downloads the report list.

b) Card Accounts’ Transfer :
The client can achieve the fund to another person’s Credit Card in the same city.

c) Bank-Securities Accounts Transfer :
The client can achieve the fund transfer between his own bank savings accounts of his own Credit Card account and his own capital account in the securities company. Moreover, the client can inquire about the present balance at real time.

d) The Transaction of Foreign Exchange:
The client can trade the foreign exchange, cancel orders and inquire about the information of the transaction of foreign exchange according to the exchange rate given by our bank on net.

e) The B2C Disbursement on Net :
The client can do the real-time transfer and get the feedback information about payment from our bank when the client does shopping in the appointed web-site.

f) Client Service :
The client can modify the login password, information of the Credit Card and the client information in e-bank on net.

g) Account Management :
The client can modify his own limits of right and state of the registered account in the personal e-bank, such as modifying his own login password, freezing or deleting some cards and so on.

131 www.businessdictionary.com/definition/electronic-banking.htm
h) Reporting the Loss of the Account:
The client can report the loss in the local area (not nationwide) when the client’s Credit Card or passbook is missing or stolen.

E-BANKING FACILITIES OFFERED BY FINANCIAL INSTITUTIONS¹³²

Online banking facilities offered by various financial institutions have many features and capabilities in common, but also have some that are application specific.

The common features fall broadly into several categories

A bank customer can perform some non-transactional tasks through online banking, including -

- viewing account balances
- viewing recent transactions
- downloading bank statements, for example in PDF format
- viewing images of paid cheques
- ordering cheque books
- download periodic account statements
- Downloading applications for M-banking, E-banking etc.
- Bank customers can transact banking tasks through online banking, including -
  - Funds transfers between the customer’s linked accounts
  - Paying third parties, including bill payments (see, e.g., BPAY) and telegraphic/wire transfers
  - Investment purchase or sale
  - Loan applications and transactions, such as repayments of enrollments
  - Register utility billers and make bill payments
  - Financial institution administration
  - Management of multiple users having varying levels of authority
  - Transaction approval process
  - the process of banking has become much faster

¹³² en.wikipedia.org/wiki/Online banking
2.2.7 RISE OF "E-BANKING" IN INDIA

Banking system plays a significant role in the society. No financial transactions are possible without support of the banks. Banks are considered as the most dependable institution in managing the money matters. Banking is the only system which provides security to our cash, which gives us money as and when required and even safe guards from fraudulent money tenders.

Indian banking industry has witnessed a tremendous developments due to sweeping changes that are taking place in the information technology. Electronic banking has emerged from such an innovative development. The most striking is its extensive reach. It is no longer confined to only metropolitans or cosmopolitans in India. In fact, Indian banking system has reached even to the remote corners of the country. This is one of the main reasons of India’s growth process.

In the past, the business operations in the traditional banking were carried out manually but with the frisky changes in the trend and with the advent of Information Technology, the concept of Electronic Banking arises all over the world. Banking today is technology driven. With technological advancement the conventional branch banking is giving way to “Anytime Anywhere Banking”.

In India e-banking is of fairly recent origin. The traditional model for banking has been through branch banking. Only in the early 1990s there has been start of non-branch banking services. The good old manual systems on which Indian Banking depended upon for centuries seem to have no place today. The credit of launching internet banking in India goes to ICICI Bank. Citibank and HDFC Bank followed with internet banking services in 1999. Several initiatives have been taken by the Government of India as well as the Reserve Bank to facilitate the development of e-banking in India.

The Government of India enacted the IT Act, 2000 with effect from October 17, 2000 which provided legal recognition to electronic transactions and other means of electronic commerce. The Reserve Bank is monitoring and reviewing the legal and other requirements of e-banking on a continuous basis to ensure that e-banking would develop on sound lines and e-banking related challenges would not pose a threat to financial stability. A high level Committee under chairmanship of Dr. K.C. Chakrabarty

133 www.theinternationaljournal.org
and members from IIT, IIM, IDRBT, Banks and the Reserve Bank prepared the „IT Vision Document- 2011-17 , for the Reserve Bank and banks which provides an indicative road map for enhanced usage of IT in the banking sector."^134

To cope with the pressure of growing competition, Indian commercial banks have adopted several initiatives and e-banking is one of them. The competition has been especially tough for the public sector banks, as the newly established private sector and foreign banks are leaders in the adoption of e-banking. Indian banks offer to their customers following e-banking products and services:

1. Automated Teller Machines (ATMs)
2. Internet Banking
3. Mobile Banking
4. Phone Banking
5. Telebanking
6. Electronic Clearing Services
7. Electronic Clearing Cards
8. Smart Cards
9. Door Step Banking
10. Electronic Fund Transfer

ADVANTAGES OF E-BANKING ^135

a) Account Information: Real time balance information and summary of days transaction. a) Fund Transfer: Manage your Supply-Chain network, effectively by using our online hand transfer mechanism. We can effect fund transfer on a real time basis across the bank locations.

b) Make a banking request online.

c) Downloading of account statements as an excel file or text file.

d) Customers can also submit the following requests online:

i) Registration for account statements by e-mail daily / weekly / fortnightly / monthly basis.

[^134]: http://www.rbi.org.in/rdoc.in/Publications
[^135]: www.academia.edu/
ii) Stop payment or cheques
iii) Cheque book replenishment
iv) Demand Draft / Pay-order
e) Opening of fixed deposit account
f) Opening of Letter of credit
j) Customers can Integrate the System with his own ERP
k) Bill Payment through Electronic Banking
l) The Electronic Shopping Mall
m) Effecting Personal Investments through Electronic Banking
n) Investing in Mutual funds
o) Initial Public Offers Online

**CHALLENGES IN ADOPTION OF E-BANKING**

E-banking is facing following challenges in Indian banking industry:

- The most serious threat faced by e-banking is that it is not safe and secure all the time. There may be loss of data due to technical defaults.
- E-banks are facing business challenges. For the transactions made through internet, the service charges are very low. Unless a large number of transactions are routed over the Web the e-banks cannot think of profit.
- There is lack of preparedness both on part of banks and customers in the adoption of new technological changes.
- There is lack of proper infrastructure for the installation of e-delivery channels.

**IMPACT OF E-BANKING ON TRADITIONAL SERVICES**

i) E-banking transactions are much cheaper than branch or even phone transactions.
ii) E-banks are easy to set up, so lots of new entrants may join.
iii) E-banking gives consumers much more choice. Consumers will be less inclined to remain loyal.
iv) Portal providers are likely to attract the most significant share of banking profits.

---

136 [http://www.academia.edu](http://www.academia.edu)
137 [www.ukessays.com › Essays › Marketing](http://www.ukessays.com › Essays › Marketing)
v) Traditional banks may simply be left with payment and settlement business
vi) Traditional banks will find it difficult to evolve.

vii) E-banking is just banking offered via a new delivery channel.

2.2.8 THE EVOLUTION OF TECHNOLOGY IN INDIAN BANKING

Information technology is one of the most important facilitators for the transformation of the Indian banking industry in terms of its transactions processing as well as for various other internal systems and processes.

The technological evolution of the Indian banking industry has been largely directed by the various committees set up by the RBI and the government of India to review the implementation of technological change. No major breakthrough in technology implementation was achieved by the industry till the early 80s, though some working groups and committees made stray references to the need for mechanization of some banking processes. This was largely due to the stiff resistance by the very strong bank employees unions. The early 1980s were instrumental in the introduction of mechanisation and computerisation in Indian banks. This was the period when banks as well as the RBI went very slow on mechanisation, carefully avoiding the use of ‘computers’ to avoid resistance from employee unions. However, this was the critical period acting as the icebreaker, which led to the slow and steady move towards large scale technology adoption.

The first blueprints of adaptation of IT in banks were drawn with the establishment of “Working Group “to consider feasibility of introducing MICR/OCR Technology for Cheque Processing under the Chairman-ship of Dr.Y.B.Damle, Adviser of Management Services Department, Reserve Bank of India.”

The technological evolution of the Indian banking industry has been largely directed by the various committees set up by the RBI and the government of India to review the implementation of technological change. No major breakthrough in technology implementation was achieved by the industry till the early 80s, though some working groups and committees made stray references to the need for mechanization of some banking processes. This was largely due to the stiff resistance by the very strong bank employees unions.

138 IBA Bulletin (Various issues)
employees unions. The early 1980s were instrumental in the introduction of mechanisation and computerisation in Indian banks. This was the period when banks as well as the RBI went very slow on mechanisation, carefully avoiding the use of ‘computers’ to avoid resistance from employee unions. However, this was the critical period acting as the icebreaker, which led to the slow and steady move towards large scale technology adoption.

In March 1987 the All India Bank Employees Association (AIBEA) and the National Confederation of Banking Employees (NCBE) signed a new settlement with the IBA, it allowed for an extension of new technology in both the operations computerized and the equipment used, the concern was largely still with ways of restricting and controlling the use of computers to protect existing staff and preserve the prospects for future staff. Electronic Fund Transfer and Delivery versus Payment systems have been introduced in banks.

From Advance Ledger Posting Machines (ALPMs) and mini computers, technology in banking moved on to MICR clearing and International interconnectivity of computers for cross border transactions (SWIFT), Electronic Data Interchange (EDI), Electronic Fund Transfer at Point of Sales (EFTPoS), Credit & Debit Cards, Automated Teller Machines (ATMs), Telephone Banking and the like. The landmark development of setting up of Indian financial Network (INFINET) a Wide Area Satellite based network based on VSAT technology is facilitating an efficient and integrated interbank payment system in the country.  

As Dr. Rangrajan has put it, in banking industry, technology is finding its use in five key areas viz, convenience in product delivery and access, managing productivity and performance, product design, adapting to market and customer needs and access to customer market. Through the most modern electronic delivery channels, banks are able to deliver their products more cheaply than the traditional branch networks loaded with expensive staff. Information Technology has enabled banks to increase the range of their products and market them more effectively. This has resulted in cutting costs of banks and improving results. Information Technology has also enabled banks to meet the new challenges of Asset Liability Management and Credit Risk Management in the

139 Reserve Bank of India, RBI Bulletin (Various issues)
new deregulated environment, through better Management Information System. The other major advantages of technology adaptation are quick and effective customer service, better housekeeping, increase in productivity and profitability, faster decision making, better operational efficiency, and increase in volume.

2.2.9 COMPUTERISATION IN PUBLIC SECTOR BANKS

Various committees like the second Rangrajan Committee, Saraf Committee, Shere Committee and the Vasudevan Committee had gone into various aspects of computerization in the banking sector. As a culmination of the implementation of the recommendations of these various committees, all large branches of banks have been computerized and banks have moved into the direction of inter-branch and interbank connectivity. The process of computerization marked the beginning of all technological initiatives in the banking industry. Computerization of bank branches had started with installation of simple computers to automate the functioning of branches, especially at high traffic branches. Thereafter, Total Branch Automation was in use, which did not involve bank level branch networking, and did not mean much to the customer.

Computerisation as well as the adoption of core banking solutions was one of the major steps in improving the efficiency of banking services. It is important to note that as on 31st March 2010 almost 98 percent of branches of public sector banks are fully computerised and within which almost 90 percent of branches are on core banking platform. As on 31st March 2013 100% Computerization & Core banking solution is implemented

Computerisation & CBS in Public Sector Banks (31st March2010)

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>FY07</th>
<th>FY08</th>
<th>FY09</th>
<th>FY10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully computerised branches(CBS and others)</td>
<td>85.6</td>
<td>93.7</td>
<td>95.0</td>
<td>97.8</td>
</tr>
<tr>
<td>Branches under CBS</td>
<td>44.4</td>
<td>67.7</td>
<td>79.4</td>
<td>90.0</td>
</tr>
<tr>
<td>Branches fully computerised(other than under CBS)</td>
<td>41.2</td>
<td>26.6</td>
<td>15.6</td>
<td>7.8</td>
</tr>
<tr>
<td>Partially computerised Branch</td>
<td>14.4</td>
<td>6.3</td>
<td>5.0</td>
<td>2.2</td>
</tr>
</tbody>
</table>

Note:-Now 100% computerisation & CBS is effected in Banking Sector

Core Banking Solutions (CBS) is the networking of the branches of a bank, the networking of branches under CBS enables centralized data management and aids in

140 http://www.rbi.org.in/rdoc.in/Publications
141 Source: Report on Trends and Progress of Banking in India, RBI, Mumbai, Various Issues
the implementation of internet and mobile banking. Besides, CBS helps in bringing the complete operations of banks under a single technological platform.

**PAPER BASED CLEARING SYSTEMS**
Among the most important improvement in paper based clearing systems was the introduction of MICR technology in the mid 1980s. Though improvements continued to be made in MICR enabled instruments, the major transition is expected now, with the implementation of the Cheque Truncation System for the processing of cheques.

### 2.2.10 DEVELOPMENT OF DISTRIBUTION CHANNELS
The major and upcoming channels of distribution in the banking industry, besides branches are ATMs, internet banking, mobile and telephone banking and card based delivery systems. Due to IT adaptation in banking, there is a market shift from conventional banking to convenience banking. ATMs have now emerged as a marketing tool to target the Indian Middle Class-the segment that provides bulk of deposits. After years of putting up with endless public holidays and bank strikes, Indians are catching up with the concept of banking 24x7 through ATMs. Off site ATM kiosks of many banks are virtual branches, as customer can conduct any transactions, through the touch screens, which will enables customers to log in and do banking net. Most banks are networking the ATMs. A network of connected ATMs of various banks (Swadhan system) is operational in Mumbai. The Shared Payment Network System (SPNS) symbolizes the use of technology for the direct improvement of customer services.\(^{142}\)

### 2.2.11 AUTOMATED TELLER MACHINES
ATMs were introduced to the Indian banking industry in the early 1990s initiated by foreign banks. Most foreign banks and some private sector players suffered from a serious handicap at that time- lack of a strong branch network.. Public sector banks have also now entered the race for expansion of ATM networks. Development of ATM networks is not only leveraged for lowering the transaction costs, but also as an effective marketing channel resource.

---

\(^{142}\) E-track June 2008 issue of Punjab National Banks Home Magazine
### INTRODUCTION OF BIOMETRICS ATMS

Banks across the country have started the process of setting up ATMs enabled with biometric technology to tap the potential of rural markets. A large proportion of the population in such centers does not adopt technology as fast as the urban centers due to the large scale illiteracy. Development of biometric technology has made the use of self-service channels like ATMs viable with respect to the illiterate population. Though expensive to install, the scope of biometrics is expanding rapidly. It provides for better security system, by linking credentials verification to recognition of the face, fingerprints, eyes or voice. Some large banks of the country have taken their first steps towards large scale introduction of biometric ATMs, especially for rural banking. At the industry level, however, this technology is yet to be adopted; the high costs involved largely accounting for the delay in adoption.

### MULTILINGUAL ATMS

Installation of multilingual ATMs has also entered pilot implementation stage for many large banks in the country. This technological innovation is also aimed at the rural banking business believed to have large untapped potential. The language diversity of India has proved to be a major impediment to the active adoption of new technology, restrained by the lack of knowledge of English.

### MULTI FUNCTIONAL ATMS

Multifunctional ATMs are yet to be introduced by most banks in India, but have already been recognized as a very effective means to access other banking services. Multifunctional

---

143 Source Report on Trends and Progress of Banking in India, RBI, Mumbai, Various Issues
144 http://www.rbi.org.in/rdoc.in/Publications
145 Ibid
146 http://www.rbi.org.in/rdoc.in/Publications
ATMs are equipped to perform other functions, besides dispensing cash and providing account information. Mobile recharges, ticketing, bill payment, and advertising are relatively new areas that are being explored via multifunctional ATMs, which have the potential to become revenue generators for the banks by effecting sales, besides acting as delivery channels. Most of the service additions to the ATM route require specific approval from the regulator.

**ATM NETWORK SWITCHES**\(^{147}\)

ATM switches are used to connect the ATMs to the accounting platforms of the respective banks. In order to connect the ATM networks of different banks, apex level switches are required that connect the various switches of individual banks. Through this technology, ATM cards of one bank can be used at the ATMs of other banks, facilitating better customer convenience. Under the current mechanism, banks owning the ATM charge a fee for allowing the customers of some other bank to access its ATM. Among the various ATM network switches are Cash Tree, BANCS, Cashnet Mitr and National Financial Switch. Most ATM switches are also linked to Visa or MasterCard gateways. In order to reduce the cost of operation for banks, IDRBT, which administers the National Financial Switch, has waived the switching fee with effect from December 3, 2007.

**2.2.12 INTERNET BANKING**

Indian banks adopted Internet banking from the early 2000s. Due to the adoption of IT technology Internet has became the most powerful instrument in Internet Banking as a reflective electronic delivery channel. Due to the adoption of technology there is a decline tend in traditional branch network and customers now prefer the transact their business on internet banking from their homes, or office using PC and browser, making Anywhere, Anytime Banking a reality.

Internet banking services are offered to the customers in three levels. On first level only queries are handled with the help of the bank’s information website; the second level which enables customers to give instructions, online applications and balance enquiries with the

\(^{147}\) Reserve Bank of India, RBI Bulletin (Various issues)
help of Simple Transactional Websites, no fund based transactions are allowed to be conducted. Third level is the fully transactional websites, which allow for fund transfers and value added services. Internet banking in India has reached to the level three. This has controlled the development of internet banking in India. Internet Banking reduces banks operating expenses and does wonders in the bottom-line of banks. It is estimated that cost per transaction in Internet banking will be only one tenth of a regular branch transaction. It has much to offer in terms of cost reduction to all customers. Successfully integrating brick less banking into a bank’s operating strategy will bring a greater challenge for banks. Internet banking can be offered only by banks licensed and supervised in India, having a physical presence in India. Overseas branches of Indian banks are allowed to undertake internet banking only after satisfying the host supervisor in addition to the home supervisor.

PHONE BANKING:- A service provided by a bank or other financial institution, that enables customers to perform financial transactions over the telephone, without the need to visit a bank branch or automated teller machine. Telephone banking times can be longer than branch opening times, and some financial institutions offer the service on a 24 hour basis.148 A customer could conduct the following transaction via Phone Banking:

i) Account Balance Information & list of latest transaction
ii) Electronic Bill Payments
iii) Funds transfers between a customers’ accounts

MOBILE BANKING: - Mobile banking is a system that allows customers of a financial institution to conduct a number of financial transactions through a mobile device such as a mobile phone or personal digital assistant. Mobile banking differs from mobile payments, which involve the use of a mobile device to pay for goods or services either at the point of sale or remotely, analogously to the use of a debit or credit card to effect an EFTPOS payment. The earliest mobile banking services were offered over SMS, a service known as SMS banking. With the introduction of smart phones with WAP support enabling the use of the mobile web in 1999, the first European banks started to offer mobile banking on this

148 http://en.wikipedia.org/wiki/Telephone_banking
platform to their customers\textsuperscript{149}

M-Banking provide the following banking services to a customer:-

- Account Balance Information & list of latest transaction
- Electronic Bill Payments
- Micro Payments
- Mobile Recharge
- Cheque Book Request
- Cheque Status
- Stop Payment Instructions
- Funds Transfer from Customer’s Accounts

The provision of real time updates of critical banking transactions is the main benefit of M-Banking- for example soon after a transactions like ATM cash withdrawal customer gets a mobile alert about it through M-Banking

**CARD BASED DELIVERY SYSTEMS**

Among the card based delivery mechanisms for various banking services, are credit cards, debit cards, smart cards etc. These have been immensely successful in India since their launch. Penetration of these card based systems have increased manifold over the past decade. Aided by expanding ATM networks and Point of Sale (POS) terminals, banks have been able to increase the transition of customers towards these channels, thereby reducing their costs too. The Smart card technology has brought a dramatic change in our daily lives. Smart card, which is a chip based card, is a kind of an electronic purse. A smart card is truly powerful financial token, which carries out all the functions of magnetic stripe cards like ATM card, credit & debit card etc\textsuperscript{150}

**SATELLITE BANKING**

Satellite banking is also an upcoming technological innovation in the Indian banking industry, which is expected to help in solving the problem of weak terrestrial communication links in many parts of the country. The use of satellites for establishing connectivity between

\textsuperscript{149} \url{http://en.wikipedia.org/wiki/Mobile_banking}
\textsuperscript{150} \url{http://www.rbi.org.in/rdoc.in/Publications}
branches will help banks to reach rural and hilly areas in a better way, and offer better facilities, particularly in relation to electronic funds transfers.\textsuperscript{151}

**CHEQUE TRUNCATION SYSTEM (CTS)**

The cheque truncation system was launched on a pilot basis in the National Capital Region of New Delhi on February 1, 2008, with the participation of 10 banks. The main advantage of the cheque truncation system is that it obviates the physical presentation of the cheque to the clearing house. Instead, the electronic image of the cheque would be required to be sent to the clearing house. This would provide a more cost-effective mode of settlement than manual and MICR clearing, enabling realization of cheques on the same day. Amendments have already been made in the Negotiable Instrumental Act to give legal recognition to the electronic image of the truncated cheque, providing for a sound legal framework for the introduction of CTS\textsuperscript{152}.

**NATIONAL ELECTRONIC FUND TRANSFER (NEFT) SCHEME**

A new variant of the EFT called the National EFT (NEFT) was decided to be implemented (November 2005) so as to broaden the facilities of EFT. NEFT provided for integration with the Structured Financial Messaging Solution (SFMS) of the Indian Financial Network (INFINET)\textsuperscript{153}.

**REALTIME GROSS SETTLEMENT**

RBI has established a Real Time Gross Settlement System (RTGS) which has brought online banking in India. By using RTGS one can directly make payment to anybody by punching in a few keys; no matter in which Bank he maintains his account.". The RTGS system also allows banks to use it for high value fund transfers (Above INR one lakh.)\textsuperscript{154}.

\textsuperscript{151} http://www.rbi.org.in/rdoc.in/Publications\textsuperscript{152} ibid\textsuperscript{153} ibid\textsuperscript{154} ibid
2.3 MEANING AND CONCEPT OF CYBER CRIMES IN BANKING

“History reveals that the Cyber crime originated even from the year 1820. That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage.”

"Cybercrime" combines the term "crime" with the root "cyber" from the word "cybernetic", from the Greek, "kubernân", which means to lead or govern.

Due to advent of Information technology it leads to advent new forms of crime & new ways to commit old forms of crime. For instance, phishing, Pharming, and viruses were completely non-existent before the arrival of the internet, while long existing crimes such as fraud, theft, and even terrorism can now all be committed in new (and sometimes easier) ways in the cyber world. Due to its decentralized structure, users of the internet can enjoy high levels of secrecy, with little risk of being traced. Consequently, the internet is a magnet for all sorts of common criminals - after all, cybercrime is just a regular crime with an "online" or "computer" aspect.

Cyber crimes are very serious threats for the present as well as times to come and pose one of the most difficult challenges before the law enforcement machinery. Most cyber crimes do not involve violence but rather greed, pride, and lack of character or even perversity of the culprit. It is difficult to identify the culprit, as the Net can be vicious web of deceit and can be accessed from any part of the globe. For these reasons cyber crimes are considered “white-collar crime”.156

155 Research paper “DETECTION OF CYBER CRIME AND INVESTIGATION” presented by Justice K.N.BASHA, Judge, Madras High Court, Chennai, in the Seminar and Workshop organised on 28.06.2010 & 29.06.2010 at Sardar Vallabhbhai Patel National Police Academy, Hyderabad.
156 Manikyam Mrs. K.Sita Dr. " Cyber Crimes" Law & policy perspectives by edition Hind Law House Pune 2009
2.3.1 CYBER CRIME- MEANING AND DEFINITION

2.3.1(A) FOOTPRINTS OF CRIME IN ANCIENT INDIA.

“Crime” is a harmful act or omission against the public which the State wishes to prevent and which, upon conviction, is punishable by fine, imprisonment or death. As per Oxford English Dictionary meaning of crime is an act punishable by law, as being forbidden by statute or injurious to the public welfare, an evil or injurious act; an offence, sin; esp. of a grave character.

The footprints of the crime are as old as human society. India’s Culture is one of the oldest of the world. As for as fiscal crimes are concerned, it is stated in “Hindu Darshanshastras” that in ancient India “Danda” was considered to be a crucial constituent of legal & social system. It was signified punishment meant for violating various laws of Society. These laws were framed and established by the ruling classes and on many points followed the principal of “Varna” or “Class Legislation”. Various Dharmashastras, material demonstrate the judiciary was not only an important arm of Government, but also indispensable to the power structure known as “State” Let us consider the position of crime and punishment in “Smriti” on ancient time in India. The “Smritis” prescribed various rules relating to punishment to be awarded for crimes.

In Kautilya’s “Arthashastra” which was written around 350 BC describes the different kinds of punishments for different offences. Kautilya’s “Arthashastra” is considered to be an authentic book in India, which discusses the different types of crimes, preventive measures to be taken by the King, This ancient book also gives the set of punishment for the list of different offences. How to recover the losses caused to the victims by the criminal has also been discussed in it.

THE FIRST RECORDED CYBER CRIME

The first recorded cyber crime took place in the year 1820 when Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard’s

---

employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber crime!159

2.3.1(B) COMPUTER CRIME & CYBER CRIME

At present time, financial transactions are performed with the help of computers. Culprits are also materialised their illegal plans with the help of computers to do harm to banks and their customers such types of crimes are known as cyber crimes. We can define it as follows:-

COMPUTER CRIME

“Computer crime” is often used to define any criminal activities that are committed against a computer or similar device, and data or program therein. In computer crimes, the computer is the target of criminal activities. The “computer” in this context refers to the hardware, but the crimes, as we shall see, more often than not relate to the software and the data or program contained within it.160

As much as the computer has been used to improve the mode of operations in the different sectors of the society, it has also evolved as a medium for some people to commit crimes. It started in the 1960’s in the form of hacking as a means of solving problems and then in the 1970s, computer crimes such as privacy violations, phone tapping, trespassing and distribution of illicit materials were experienced. Software piracy, copyright violations, and the introduction of viruses were added to the list in the 1980s. Things went downhill and now, the extent of the damage caused by computer crimes is enormous; the international market has not been left out with computers being used for espionage and transnational organized crime and terrorism. Computer crimes have become a major source of concern for organizations worldwide161.

159 Source: www.inf.tsu.ru/Web design/Libra3.nsf/.../$FILE/cybercrime.pdf
160 Warren B. Chik, Assistant Professor of Law, Singapore Management University in his article “Challenges to Criminal Law Making in the New Global Information Society”
161 Journal of Internet Banking and Commerce JIBC April 2010, Vol. 15, No.1 - 1
Source: http://www.arraydev.com/commerce/jibc/
**CYBER CRIME**

Crime is an aspect of society that adversely affects one and all. Cyber-crime is a recent addition to the list of crimes that affect the society, whether directly or indirectly. In recent past, cyber crime has increased at very terrific rate, due to the rapid utilization of the Internet and the computerisation of activities in all walk of the life. “Cyber crime” is an activity committed using the Internet or computer or other electronic devices as the medium, in violation of existing laws for which punishment is imposed upon successful conviction. Cyber crime also includes the use of digital resources to commit traditional crimes such as theft of identifiable information and other forms of proprietary information or property in both digital and physical form. ¹⁶²

With the advent of computers (and especially the Internet) businesses are subject to threats of malicious activities and cyber-crimes. Cyber criminals use computers and technology to carry out the destructive activities that have been around for decades. Whether it is insiders or unknown intruders involved in hacking (i.e. the unauthorized use or attempt to circumvent the security mechanisms of an information system or network), cracking (i.e., breaking into a computer system), phishing (i.e., attempting to acquire identifiers and passwords), or phreaking (i.e., cracking a phone or communication network), as long as people are the weakest link, there really is no safe harbour from cybercrime. In the present era of rapid growth, information technology is surrounding all walks of life in all over the world. The effect of the technology is so deep that man cannot spend a day without computers or a mobile. ¹⁶³

**2.3.1(C) DEFINITION OF CYBER CRIME**

Cyber crime is not defined anywhere in Information Technology Act 2000, I.T. Amendment Act 2008 and in any other legislation in India. Offence or crime has been dealt with elaborately listing various acts and the punishments for each, under the Indian Penal Code, 1860 and quite a few other legislations too.

The term ‘cyber crime’ has not been defined in any Statute or Act. However, following

---

¹⁶² Warren B. Chik, Assistant Professor of Law, Singapore Management University in his article “Challenges to Criminal Law Making in the New Global Information Society”

¹⁶³ ibid
definitions are available.

**The Oxford Reference Online defines 'cyber crime'** as crime committed over the Internet. The Encyclopedia Britannica defines 'cyber crime' as any crime that is committed by means of special knowledge or expert use of computer technology.

**CBI Manual defines cyber crime as:**
Crimes committed by using computers as a means, including conventional crimes. (Crimes in which computers are targets.

**United Nations' Definition of Cyber Crime:**
At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cyber crime was broken into two categories and defined as:

**Cyber Crime in a narrow sense (computer crime):** Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

**Cyber Crime in a broader sense (computer-related crime):** Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

Of course, these definitions are complicated by the fact that an act may be illegal in one nation but not in another. There are more concrete examples, including

1) Unauthorized access
2) Damage to computer data or programs
3) Computer sabotage
4) Unauthorized interception of communications
5) Computer espionage

These definitions, do give us a good starting point for determining just what we mean by the term cyber crime. 164

**Hence, to define cyber crime,** we can say, it is just a combination of crime and computer. To put it in simple terms 'any offence or crime in which a computer is used is a cyber crime'

The I.T. Act defines a computer, computer network, data, information and all other

---

164 Cyber Law & Information Technology by Talwant Singh Addl. Distt. & Sessions Judge, Delhi
necessary ingredients that form part of a cyber crime, about which we will now be discussing in detail. In a cyber crime, computer or the data itself the target or the object of offence or a tool in committing some other offence, providing the necessary inputs for that offence. All such acts of crime will come under the broader definition of cyber crime.\textsuperscript{165} 

A generalized definition of cyber crime may be "unlawful acts wherein the computer is either a tool or target or both". Cyber Crime could reasonably include a wide variety of criminal offences and activities.

2.3.1(D) NATURE OF CYBER CRIME

The term ‘cyber’ is derived from the word ‘cybernetics' which means science of communication and control over machine and man. Cyberspace is the new horizon which is controlled by machine for information and communication between human beings across the world. Therefore, crimes committed in cyberspace are to be treated as cyber crimes. In wider sense, cyber crime is a crime on the Internet which includes hacking, terrorism, fraud, gambling, cyber stalking, cyber theft, cyber pornography, flowing of virus etc. Cyber crimes are computer related as well as computer generated crimes. It is increasing every moment which is the cause of global tension. Therefore, law enforcing agencies must have detail knowledge and understanding about varying nature of cyber crime.

Though there is nothing new in the adoption of new technologies by criminals. In the era of liberalization and globalization we must recognize cyber crime as significantly new phenomenon which has political, social and economic impact worldwide. Cyber crime is a threat to national and international socio-economic political and security system

CHARACTERISTICS OF CYBER CRIME

Following are the main characteristics of cybercrime

1. Low risk high rewarding ventures
2. Lack of awareness among victims
3. Physical presence not required
4. Lack of hi-tech skills among investigating agencies
5. Victims refrain from reporting cases
6. No violence is involved.

7. No territorial boundaries.
8. Anonymity and Openness
9. Paucity of authentic evidence
10. Have wider ramifications

2.3.2 GLOBAL CYBER CRIME SCENARIO

At the global level, law enforcement respondents to the study perceive increasing levels of cybercrime, as both individuals and organized criminal groups exploit new criminal opportunities, driven by profit and personal gain. Cybercrime is a rampant problem, striking 65 percent of Internet users worldwide according to a new study released by security vendor Symantec. Web surfers have fallen victim to such cybercrimes as computer virus, online credit card fraud, online scams, social networking profile hacking, and identity theft. Malware, or computer virus attacks, which have affected just over half of all respondents, are the most common form of cybercrime, according to the survey. However, only 10% of adults said they’ve been victims of online scams, and only 7% have fallen prey to credit card fraud.

SYMANTEC CYBER CRIME- TOP 20 COUNTRIES 166

Symantec has ranked 20 countries that face, or cause, the most cyber crime. In compiling such a list, Symantec was able to quantify software code that interferes with a computer’s normal functions, rank zombie systems, and observe the number of websites that host phishing sites, which are designed to trick computer users into disclosing personal data or banking account information. Symantec was also able to obtain data including the number of bot-infected systems which are those controlled by cyber criminals, rank countries where cyber attacks initiated and factor in the a higher rate of cyber crime in countries that have more access to broadband connections. The highest rate of cyber crime was found to be in the United States which may mainly contribute to the broad range of available broadband connections, which are those that allow uninterrupted internet connectivity. All of the contributing factors allowed Symantec to effectively rank a top 20 list of countries that have the most cyber crime.

166 Source: http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/
Each country lists six contributing factors to substantiate its cyber crime ranking as under:


### Ranking of Top 20 Countries with highest rate of Cyber Crime

<table>
<thead>
<tr>
<th>Rank</th>
<th>Name of Country</th>
<th>Share of Malicious Computer Activity</th>
<th>Malicious Code Rank,</th>
<th>Spam Zombies Rank,</th>
<th>Phishing Web Site Hosts Rank</th>
<th>Bot Rank</th>
<th>Attack Origin Rank,</th>
</tr>
</thead>
<tbody>
<tr>
<td>1&lt;sup&gt;st&lt;/sup&gt;</td>
<td>U. S.A</td>
<td>23%</td>
<td>1%</td>
<td>3%</td>
<td>1%</td>
<td>2%</td>
<td>1%</td>
</tr>
<tr>
<td>2&lt;sup&gt;nd&lt;/sup&gt;</td>
<td>China</td>
<td>9%</td>
<td>2%</td>
<td>4%</td>
<td>6%</td>
<td>1%</td>
<td>2%</td>
</tr>
<tr>
<td>3&lt;sup&gt;rd&lt;/sup&gt;</td>
<td>Germany</td>
<td>6%</td>
<td>12%</td>
<td>2%</td>
<td>2%</td>
<td>4%</td>
<td>4%</td>
</tr>
<tr>
<td>4&lt;sup&gt;th&lt;/sup&gt;</td>
<td>Britain</td>
<td>5%</td>
<td>4%</td>
<td>10%</td>
<td>5%</td>
<td>9%</td>
<td>3%</td>
</tr>
<tr>
<td>5&lt;sup&gt;th&lt;/sup&gt;</td>
<td>Brazil</td>
<td>4%</td>
<td>16%</td>
<td>1%</td>
<td>16%</td>
<td>5%</td>
<td>9%</td>
</tr>
<tr>
<td>6&lt;sup&gt;th&lt;/sup&gt;</td>
<td>Spain</td>
<td>4%</td>
<td>10%</td>
<td>8%</td>
<td>13%</td>
<td>3%</td>
<td>6%</td>
</tr>
<tr>
<td>7&lt;sup&gt;th&lt;/sup&gt;</td>
<td>Italy</td>
<td>3%</td>
<td>11%</td>
<td>6%</td>
<td>14%</td>
<td>6%</td>
<td>8%</td>
</tr>
<tr>
<td>8&lt;sup&gt;th&lt;/sup&gt;</td>
<td>France</td>
<td>3%</td>
<td>8%</td>
<td>14%</td>
<td>9%</td>
<td>10%</td>
<td>5%</td>
</tr>
<tr>
<td>9&lt;sup&gt;th&lt;/sup&gt;</td>
<td>Turkey</td>
<td>3%</td>
<td>15%</td>
<td>8%</td>
<td>24%</td>
<td>5%</td>
<td>12%</td>
</tr>
<tr>
<td>10&lt;sup&gt;th&lt;/sup&gt;</td>
<td>Poland</td>
<td>3%</td>
<td>23%</td>
<td>9%</td>
<td>8%</td>
<td>7%</td>
<td>17%</td>
</tr>
<tr>
<td>11&lt;sup&gt;th&lt;/sup&gt;</td>
<td>India</td>
<td>3%</td>
<td>3%</td>
<td>11%</td>
<td>22%</td>
<td>20%</td>
<td>19%</td>
</tr>
<tr>
<td>12&lt;sup&gt;th&lt;/sup&gt;</td>
<td>Russia</td>
<td>2%</td>
<td>8%</td>
<td>7%</td>
<td>7%</td>
<td>17%</td>
<td>14%</td>
</tr>
<tr>
<td>13&lt;sup&gt;th&lt;/sup&gt;</td>
<td>Canada</td>
<td>2%</td>
<td>5%</td>
<td>40%</td>
<td>3%</td>
<td>14%</td>
<td>10%</td>
</tr>
<tr>
<td>14&lt;sup&gt;th&lt;/sup&gt;</td>
<td>South Korea</td>
<td>2%</td>
<td>21%</td>
<td>19%</td>
<td>4%</td>
<td>15%</td>
<td>7%</td>
</tr>
<tr>
<td>15&lt;sup&gt;th&lt;/sup&gt;</td>
<td>Taiwan</td>
<td>2%</td>
<td>11%</td>
<td>21%</td>
<td>12%</td>
<td>11%</td>
<td>15%</td>
</tr>
<tr>
<td>16&lt;sup&gt;th&lt;/sup&gt;</td>
<td>Japan</td>
<td>2%</td>
<td>7%</td>
<td>29%</td>
<td>11%</td>
<td>22%</td>
<td>11%</td>
</tr>
<tr>
<td>17&lt;sup&gt;th&lt;/sup&gt;</td>
<td>Mexico</td>
<td>2%</td>
<td>6%</td>
<td>18%</td>
<td>31%</td>
<td>21%</td>
<td>16%</td>
</tr>
<tr>
<td>18&lt;sup&gt;th&lt;/sup&gt;</td>
<td>Argentina</td>
<td>1%</td>
<td>44%</td>
<td>12%</td>
<td>20%</td>
<td>12%</td>
<td>18%</td>
</tr>
<tr>
<td>19&lt;sup&gt;th&lt;/sup&gt;</td>
<td>Australia</td>
<td>1%</td>
<td>14%</td>
<td>37%</td>
<td>17%</td>
<td>27%</td>
<td>13%</td>
</tr>
<tr>
<td>20&lt;sup&gt;th&lt;/sup&gt;</td>
<td>Israel</td>
<td>1%</td>
<td>40%</td>
<td>16%</td>
<td>15%</td>
<td>16%</td>
<td>22%</td>
</tr>
</tbody>
</table>

Website: http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/
2.3.3 GENERAL CYBER CRIME SCENARIO IN INDIA

Cyber Crimes are a new class of crimes to India which are rapidly growing due to extensive use of internet & IT Enabled Services. The Information Technology (IT) Act, 2000, specifies the acts made punishable. Since the primary objective of this Act is to create an enabling environment for commercial use of I.T., certain omissions and commissions of criminals while using computers have not been included. Several offences having bearing on cyber-arena are also registered under the appropriate sections of the IPC with the legal recognition of Electronic Records and the amendments made in several section of IPC vide IT Act, 2000.

Another major concern with cyber crimes is its low detection level and next to negligible prosecution. The monetary loss due to information theft is impossible to assess as it depends upon the nature of information stolen. However, such losses can neither be recovered through insurance coverage nor is the law able to protect from such incidents.

According to the Norton’s Cyber Crime Report,

1) There are about 1 million cyber crimes occurring every day across the globe.
2) The total number of victims were estimated at 431 million of which 29.9 million were in India.
3) In India it is estimated that 80% of online adults have been victims in the last year. (Estimated Netizens population is therefore 37 million). The victim hood percentage is higher in India than the global figure which was 69%.

4) The direct financial cost is estimated at US $114 billion globally while it is US $ 4 billion in India. (Rs 34110 cores) The survey also estimates an indirect cost in terms of time and efforts for recovery which is placed at US$274 billion globally and US $ 3.6 billion in India.

It is interesting to note that in India the indirect costs are less than the direct costs where as the global scenario is different. This may be the result of victims not pursuing the recovery. Out of the total number of crimes,

1) Viruses accounted for 60% in India and 54% globally,
2) Online scams accounted for 20% in India and 11% globally and
3) Phishing accounted for 19% in India and 10% globally.

The report also suggests that 17% of the Crime relate to mobiles. This is quite alarming considering that the use of Mobiles for financial transactions is expected to grow exponentially in the coming years and hence the losses on mobile crimes are also likely to increase.168

During the NASSCOM Global Leadership Awards, India’s home minister revealed that India is ranked fifth in the number of cyber crimes. Every year, cyber crime in India is going up by 50 per cent and during the last five years, around 9,000 Indian websites were hacked. Major cyber crimes reported in India are denial of services, defacement of websites, SPAM, computer viruses and worms, pornography, cyber squatting, cyber stalking and phishing particularly relates to banking sector.169

---

168 By Naavi posted on 10/09/2011

169 Risk Survey 2012 conducted by FICCI&PINKERTON
## 2.3.3(A) REPORT PUBLISHED BY NATIONAL CRIME RECORD BUREAU, MINISTRY OF HOME AFFAIRS, GOVT. OF INDIA ON CYBER CRIME CASES REGISTERED (2003-2012)

### Table 2.9 - NCRB Report on Cyber Crime Cases registered (2003-2012)

<table>
<thead>
<tr>
<th>S.N.</th>
<th>Crime Head</th>
<th>Cases Registered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tampering computer source documents</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>Hacking with computer system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>i) Loss/damage to computer resource/utility</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>ii) Hacking</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>Obscene Publications/transmission in electronic form</td>
<td>20</td>
</tr>
<tr>
<td>4</td>
<td>Failure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>i) Of compliance of Certifying Authority</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ii) To assist in decrypting the information intercepted by Govt. Agency</td>
<td>6</td>
</tr>
<tr>
<td>5</td>
<td>Un-authorized access/attempt to access to protected computer system</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>Obtaining license or Digital Signature Certificate by misrepresentation/ suppression of fact</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>Publishing false Digital Signature Certificate</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>Fraud Digital Signature Certificate</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>Breach of confidentiality/privacy</td>
<td>3</td>
</tr>
<tr>
<td>10</td>
<td>Other</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>60</td>
</tr>
</tbody>
</table>

Going by the 2012 NCRB figures, there were 2876 cases registered under IT Act during the year 2012 as compared to 1791 cases during the previous year (2011) thereby reporting an increase of 60.58% in 2012 over 2011. Among these 2,876 crimes reported most of the cases are of tampering computer source (1,440) and hacking of data (435). Variation in tempering data over 2011 is 74% and hacking is 177.1% which is almost double and is alarming issue to concentrate. Crime cell is also working its level best as persons arrested in 2011 for hacking crime was 65 and in 2012 are 137 for total 435 cases recorded. But there is also little bit relief because the cases registered under categories of un-authorized

170 Chapter 18 of Report published by National Crime Record Bureau, Ministry of Home Affairs, GOI
attempt to access protected computer system decreases by 40% and decrease in cases registered under publishing false digital signature certificate, fraud digital signature certificate are 66.7% and (-)16.7% respectively. Although there is decrease in cases registered in above mentioned three categories but offenders are sharper as persons arrested under category of unauthorized attempt to access computer system in 2011 were 15 for 5 cases registered but in 2012 persons arrested for same category were 1 for 3 cases registered. No person was arrested for publishing false digital signature certificate for one case registered under IT act 2000. Total cases registered under IT act 2000 was 2,876 in 2012. When state wise observations was carried out Maharashtra state was on first place where 471 cases was registered followed by Andhra Pradesh(429), Karnataka(412), Kerala(269) and Uttar Pradesh(205) cases was registered. Number of loss/damage to computer resources and hacking cases is almost 50% of total cases. In Andhra Pradesh (292) cases was registered, Karnataka (219), Maharashtra (192), West Bengal (101) If I discuss about persons arrested in various crime cases total 1,552 persons was arrested under IT act 2000 as compared to 1,184 persons arrested in 2011. So increase in percentage over 2011 is 28.5%. Among 1,552 persons arrested 324 were from Maharashtra, Andhra Pradesh (170). Maximum number was reported from these two states.

2.3.3(B) CYBER CRIME IN BANKING INDUSTRY- A GLOBAL SCENARIO

These are challenging times for the banking industry globally, thought provoking and extremely rewarding at the same time. Due to volatile geopolitical and global macroeconomic conditions, many financial institutions have been forced to evaluate their current operating practices and think about where they would like to be in future and more importantly, how to manage growth as well as risk management in line with stakeholder expectations. In financial domain, technology is no longer an enabler, but a business driver. In last decade phenomenal growth of IT, mobile penetration and communication network has facilitated growth in extending financial services to masses. Technology has facilitated delivery of banking services to masses and changed the way of functioning of financial

---

institutions. Technology made banking services affordable and accessible by optimizing the way these institutions operate today. Regulatory bodies, banks and other institutions/agencies have taken paradigm shift in areas of respective operations, service delivery and consumer satisfaction. Financial institutions gained efficiency, outreach, spread through technology in last two decades. The benefits of technology such as scale, speed and low error rate are also reflecting in the performance, productivity and profitability of banks, which have improved tremendously in the past decade. Technology initiatives are taken by banks in the areas of financial inclusion, mobile banking, electronic payments, IT implementation and management, managing IT risk, internal effectiveness, CRM initiatives and business innovation.172

**HIGH LIGHTS OF CYBER CRIMES AGAINST BANKING SECTOR**173

As per “Symantec Cyber Crime Report 2011”

1) Currently, there are nearly 2 billion internet users and over 5 billion mobile phone connections worldwide.

2) Everyday, 294 billion emails and 5 billion phone messages are exchanged.

3) 50,000 Victims every hour

4) 820 Victims every minute

5) 14 Victims every second

**TIME AND MONEY SPENT BANKING RELATED CYBER CRIME**174

Global Scenario

USD 114 Billion is total loss of cash in 12 months

USD 274 Billion is the total loss of time for victims of cyber crime

On an average, 10 days were spent by victims to satisfactorily resolve hassles of cyber crime).

---

172 Cybercrimes - A Financial Sector View - KPMG

173 Symantec Cyber Crime Report 2011

174 Symantec Cyber Crime Report 2011
2.3.3(C) CYBER CRIME IN BANKING INDUSTRY-INDIAN SCENARIO
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 ‘hi-tech 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.

a) Cyber Crimes Increasing with Rising of E-Banking in India
India is vulnerable to cyber crimes as 97% of Indians, who use information technology, are not aware of how to be secure. The people need to be made aware this as many get E-mails as if they are coming from their banks to ask their account IDs and passwords for verification purposes. They should divulge information because this personal information can be used by cyber criminals, who sent the E-mails and in turn money could be withdrawn from their account.

b) Time and Money spent in Banking related Cyber crimes- An Indian Scenario
USD 4 billion is the total loss of cash in 12 months
USD 3.6 billion is the total loss of time for victims of cyber crime
On an average 15 days were spent by victims to satisfactorily resolve hassles of cyber crime

2.3.4 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 22nd February 2013 replied in the following manner:
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 & Credit Cards Retrieved from www.rbi.org.in (2013) and put in order as per sector wise i.e Public Sector Banks, Private Sector Bank & Foreign Banks in India

176 Symantec Cyber Crime Report 2011
177 Press Information Bureau of India Ministry of Finance published the news on 26th February 2013
Table 2.10-Cyber Frauds in Scheduled Commercial Banks (2009-2012)(Amt.in Lakh)

<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>

2.3.4(A) CYBER FRAUD CASES IN COMMERCIAL BANKS (2009-2012)

Table 2.11-, Group wise Cyber Fraud Cases in Commercial Banks (2009-2012)

<table>
<thead>
<tr>
<th>Particulars</th>
<th>No. of Cyber Crime Cases</th>
<th>Amount Involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nationalised Banks</td>
<td>94</td>
<td>152</td>
</tr>
<tr>
<td>State Bank Group</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Private Sector Banks</td>
<td>16100</td>
<td>10130</td>
</tr>
<tr>
<td>Foreign Banks</td>
<td>5769</td>
<td>4733</td>
</tr>
<tr>
<td>Total</td>
<td>21966</td>
<td>15018</td>
</tr>
</tbody>
</table>

OBSERVATION ON INTRA SECTOR BANKS (Public, Private & Foreign Banks)

1) Number of cases during the period 2009-2012

a) In Nationalised banks no. of cases were 94 in 2009 were increased to154 cases in 2010. In 2011 no. of cases were reduced to 110 while in 2012 the no. of cases again increased to 188. It shows the increasing trend in cases of cyber crime over the years except in 2011.

b) In State Bank & its subsidiaries no. of cases were 3 in 2009. There were no increases of no. of cases in 2010 as it stood constant and showing no. of cases to the tune of 3. In 2011 the cases were suddenly increased to 18 while in 2012 the no. of cases duped to 12. It shows the increasing trend in cases of cyber crime over the year except in 2010 & 2012.

c) In Private Sector Banks no. of cases were 16100 in 2009 were reduced to 10132 in 2010. In 2011 the cases were reduced to 6527 while in 2012 cases were came down to 8322.

---

179 Lok Sabha Unstarred Question No. 2398 answered On the March 19, 2013 by Namo Narayan Meena State Finance Minister
180 http://www.rbi.org.in/rdoc.in/Publications
d) In Foreign Banks no. of cases were 57698 in 2009 were reduced to 4733 in 2010. In 2011 no. of cases were came down to 2933 while in 2012 no. of cases were touched to 3978.

2) Amount involved in cyber crime cases during the period 2009-2012

a) In Nationalised banks amount involved in 2009 was Rs.98.35 lakh. It was increased to Rs.368.65 lakh in 2010, Rs.500.29 lakh in 2011 & Rs.689.35 lakh in 2012. This shows an increasing trend over the years.

b) In State Bank & its subsidiaries amount involved in 2009 was Rs.7.46 lakh. It was came down to Rs.1.16 lakh in 2010 but again increased to Rs.172.19 lakh in 2011 & again decreased to Rs.134.46 lakh in 2012. This shows the fluctuations but an increasing trend over the years 2009

c) In Private Sector amount involved in 2009 was Rs.4232.61 lakh. It was came down to Rs.2226.25 lakh in 2010 & Rs.1670.72 lakh in 2011 but again increased to Rs.2506.67 lakh in 2012.

d) In Foreign Banks amount involved in 2009 was Rs.2894.89 lakh. It was came down to Rs.1452. lakh in 2010 & Rs.1328.99 lakh in 2011 but increased to Rs.1936.67 lakh in 2012.

From the above it reveals that State Bank Group has shown the negligible rise in no. of cases of cyber crimes and amount involved therein. Nationalised Banks are in the same category. It depicts that there is strict control & watch over the cyber crimes against e-banking in Public Sector Banks (Nationalised & State Bank Group) whereas Private Sector Banks followed by Foreign Banks operating in India have shown soaring mount in number of cases of cyber crimes & amount involved therein as compared to their counterpart Nationalised Banks & State Bank Group

1) No of Cyber Crime cases are showing the tumbled trend over the previous years from 2010 to 2012

2) Amount involved is also showing the tumbled trend over the last year except in 2012.

3) In term of percentage number of cases tumbled by 31.63% in 2010, 36.16% in 2011 and 13.2% in 2012

4) The Amount involved also tumbled by 44.02% in 2010 & 9.3% in 2011, but in 2012 it increased by 43.42%

5) No. of Cyber Crime cases & Amount involved showing the decreasing trend as on 2012
6) In term of percentage number of cases tumbled by 62.11% in 2012 over 2009 while Amount involved tumbled by 27.18% in 2012 over 2009.

2.3.4(B) CYBER FRAUD CASES IN PUBLIC SECTOR BANK (2009-2012)

I) NATIONALISED BANKS FUNCTIONING IN INDIA

Table 2.12 - Cyber Fraud Cases in Public Sector Banks (Nationalized Bank) (Amt. in Lakh)

<table>
<thead>
<tr>
<th>S.N.</th>
<th>Bank Name</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No. of Cases</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</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Andhra Bank</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>Bank of Baroda</td>
<td>6</td>
<td>5</td>
<td>12.40</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>Bank of India</td>
<td>5</td>
<td>2</td>
<td>14.61</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>Bank of Maharashtra</td>
<td>4</td>
<td>4</td>
<td>4.69</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>Canara Bank</td>
<td>6</td>
<td>1</td>
<td>62.45</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>Central Bank of India</td>
<td>2</td>
<td>2</td>
<td>2.15</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>Corporation Bank</td>
<td>2</td>
<td>2</td>
<td>6.21</td>
<td>5</td>
</tr>
<tr>
<td>9</td>
<td>Dena Bank</td>
<td>0</td>
<td>1</td>
<td>2.07</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>IDBI Bank Limited</td>
<td>24</td>
<td>13</td>
<td>15.29</td>
<td>50</td>
</tr>
<tr>
<td>11</td>
<td>Indian Bank</td>
<td>0</td>
<td>1</td>
<td>1.41</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>Indian Overseas Bank</td>
<td>2</td>
<td>3</td>
<td>1.44</td>
<td>10</td>
</tr>
<tr>
<td>13</td>
<td>Oriental Bank of Comm.</td>
<td>0</td>
<td>1</td>
<td>4.75</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>Punjab National Bank</td>
<td>33</td>
<td>108</td>
<td>248.64</td>
<td>28</td>
</tr>
<tr>
<td>15</td>
<td>Syndicate Bank</td>
<td>2</td>
<td>1</td>
<td>2.32</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>UCO Bank</td>
<td>2</td>
<td>1</td>
<td>1.60</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>Union Bank of India</td>
<td>5</td>
<td>7</td>
<td>19.22</td>
<td>2</td>
</tr>
<tr>
<td>18</td>
<td>United Bank of India</td>
<td>1</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>19</td>
<td>Vijaya Bank</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Grand Total</td>
<td>94</td>
<td>152</td>
<td>368.65</td>
<td>110</td>
</tr>
</tbody>
</table>
II) CYBER FRAUD CASES IN STATE BANK OF INDIA & ITS SUBSIDIARIES

Table 2.13- Cyber Fraud Cases in Public Sector Banks(SBI Group)(Amount. in Lakh)\textsuperscript{181}

<table>
<thead>
<tr>
<th>S.N.</th>
<th>Bank Name</th>
<th>2009 No. of Cases</th>
<th>Amount Involved</th>
<th>2010 No. of Cases</th>
<th>Amount Involved</th>
<th>2011 No. of Cases</th>
<th>Amount Involved</th>
<th>2012 No. of Cases</th>
<th>Amount Involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</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>2</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>3</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>4</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>5</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>6</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>7</td>
<td>State Bank of Travancore</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></td>
<td><strong>Grand Total</strong></td>
<td><strong>3</strong></td>
<td><strong>7.46</strong></td>
<td><strong>3</strong></td>
<td><strong>1.16</strong></td>
<td><strong>18</strong></td>
<td><strong>172.19</strong></td>
<td><strong>12</strong></td>
<td><strong>134.46</strong></td>
</tr>
</tbody>
</table>

**Public Sector Banks:** It is observed from the above that the number of cases in Nationalised Banks & State Bank Group were very meager but they went up & mounted during the period 2009 to 2012 with a little slanting in 2011. In the year 2009, PNB recorded the substantial growth of cyber crime cases afterward IDBI bank. In 2010, PNB recorded highest number of cases afterward IDBI, but amount wise, PNB was ahead of Andhra Bank, Union Bank of India and IDBI respectively. IDBI was highest afterward PNB in 2011 in terms of cases, but in terms of amount wise, IOB, PNB and Bank of Patiala registered a substantial growth. In 2012, IDBI topped the list. Afterward are Corporation Bank and PNB. IDBI, Bank of Maharashtra and PNB recorded highest positions respectively in respect of amount involved.

\textsuperscript{181} \url{http://www.rbi.org.in/rdoc.in/Publications}
2.3.4(C) CYBER FRAUD PRIVATE SECTOR BANKS

Table 2.14 - Cyber Fraud Cases in Private Sector Banks (Old & New) (Amount in Lakh)\(^{182}\)

<table>
<thead>
<tr>
<th>S.N.</th>
<th>Bank Name</th>
<th>2009 No. of Cases</th>
<th>Amount Involved</th>
<th>2010 No. of Cases</th>
<th>Amount Involved</th>
<th>2011 No. of Cases</th>
<th>Amount Involved</th>
<th>2012 No. of Cases</th>
<th>Amount Involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Axis Bank Ltd.</td>
<td>20</td>
<td>110.58</td>
<td>14</td>
<td>44.59</td>
<td>23</td>
<td>209.59</td>
<td>85</td>
<td>1225.41</td>
</tr>
<tr>
<td>2.</td>
<td>Development Credit Bank</td>
<td>2</td>
<td>0.96</td>
<td>2</td>
<td>0.30</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>3.</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>4.</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>5.</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>6.</td>
<td>ICICI Bank Ltd.</td>
<td>15666</td>
<td>3731.95</td>
<td>9811</td>
<td>1920.28</td>
<td>6013</td>
<td>1096.67</td>
<td>3428</td>
<td>676.51</td>
</tr>
<tr>
<td>7.</td>
<td>Bank of Rajasthan Ltd. (Merged With ICICI)</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>8.</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>9.</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>10.</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>11.</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>12.</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>13.</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>14.</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>15.</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></td>
<td>Grand Total</td>
<td>16100</td>
<td>4232.61</td>
<td>10130</td>
<td>2226.25</td>
<td>6527</td>
<td>1670.72</td>
<td>4144</td>
<td>2506.47</td>
</tr>
</tbody>
</table>

Private Sector Banks: It reveals from the above that private sector banks is having the lions share in cyber crimes against e-banking amount wise as well as number of cases. There was a slanting trend amount wise as well as number of cases over the years. The number of cases dropped down from 16100(2009) to 4144(2012). Similarly the amount is also dropped down from 4232.61 lakh (2009) to 1670.72 (2011), but it again went up to 2506.47Lakhs in 2012. ICICI bank topped the list afterward HDFC and Axis Banks.

\(^{182}\) http://www.rbi.org.in/rdoc.in/Publications
2.3.4(D) CYBER FRAUD CASES IN FOREIGN BANKS

Table 2.15 Cyber Fraud Cases in Foreign Banks (Amt in Lakh)

<table>
<thead>
<tr>
<th>S.N.</th>
<th>Bank Name</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>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>Ameican Express Banking Corporation</td>
<td>980</td>
<td>904.57</td>
<td>819</td>
<td>360.75</td>
</tr>
<tr>
<td>2.</td>
<td>Barclays Bank PLC</td>
<td>35</td>
<td>21.68</td>
<td>48</td>
<td>8.38</td>
</tr>
<tr>
<td>3.</td>
<td>Citi Bank N.A.</td>
<td>1226</td>
<td>773.18</td>
<td>925</td>
<td>521.27</td>
</tr>
<tr>
<td>4.</td>
<td>Deutche Bank (Asia)</td>
<td>61</td>
<td>116.64</td>
<td>35</td>
<td>81.94</td>
</tr>
<tr>
<td>5</td>
<td>Firstrand Bank</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>6.</td>
<td>Hongkong &amp; Shanghai Banking Corp. Ltd</td>
<td>3093</td>
<td>722.45</td>
<td>2520</td>
<td>293.02</td>
</tr>
<tr>
<td>7.</td>
<td>Standard Chartered Bank</td>
<td>374</td>
<td>356.37</td>
<td>386</td>
<td>187.52</td>
</tr>
<tr>
<td></td>
<td>Grand Total</td>
<td>5769</td>
<td>2894.89</td>
<td>4733</td>
<td>1452.88</td>
</tr>
</tbody>
</table>

Foreign Banks: It reveals from the above that cyber crime cases were also registered during last four years in Foreign Banks operating in India to the great degree. The data shows the decline trend in number of cases as well as amount involved over the years from 2009 till 2011. But in 2012 there was a sudden rise in number of cases as well as amount involved over 2011. From the above we could safely conclude that HSBC, which was the top bank in 2009 in terms of cases & amount involved, has came down in 2012 while Citibank and American Express have exceeded HSBC in terms of number cases as well as amount involved in reported cyber crimes.

http://www.rbi.org.in/rdoc.in/Publications
At the age of digital era, Information Technology is a very powerful instrument. Banks & other Financial Institutions are playing the important role in the Indian economy. Therefore these institutions are termed as the backbone of the economy. At this juncture, Indian Banking Industry is facing the challenges of an IT revolution. Almost all the banks in India have adopted IT solutions for rendering the banking services to their customers by using the IT tools & techniques to fulfill the needs of the customers. Due to the adoption of IT in Banks, the manual operations are negligible and maximum banking operations are performed through IT solutions. Due to the dawn of e-banking, conventional banking has been disappeared from the Indian banking panorama. In this day and age, banks have shifted from traditional banking to Core Banking Solutions Banking, which confirm the impact of IT on banks.

The increasing use of technology, particularly by Indian banks to drive its operations and to deliver world class services has lead to the evolution of a new threat. The Indian banking industry, almost in keeping with the considerate commercial approach of the country’s business, has come to the present stage. Rapid strides in Information Technology (IT) and its swift adoption by the commercial banks in India have enabled banks to use IT extensively to offer products and services to customers apart from automating internal processes. E- Banking is nothing more than traditional banking services delivered through an electronic communication, viz, Internet. These banking technologies have it’s own merits & demerits. The merits of the technology are “Benefits and Advantages” but the demerits of the technology are named as “Cyber Crime”.

These developments in banking technology for the benefit of the people have also brought opportunities for criminal activity. This is done through many methods by using internet either computers or mobile phones. Such types of crimes are termed as Cyber Crimes against E-Banking.
2.4.1 CLASSIFICATION OF CYBER CRIME

Cyber crimes have been classified on the basis of the nature and purpose of the offence and have been grouped into four categories as under:

2.4.1(A) CYBER CRIMES AGAINST PERSONS¹⁸⁴:

There are certain offences which affect the person are classified as under:

**Harassment via E-Mails**: It is very common type of harassment through sending letters, attachments of files & folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Face book, Twitter etc. increasing day by day.

**Cyber-Stalking**: It means expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.

**Dissemination of Obscene Material**: It includes Indecent exposure/ Pornography (basically child pornography), hosting of web site containing these prohibited materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.

**Defamation**: It is an act of imputing any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.

**Hacking**: It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programmes. Hackers usually hacks telecommunication and mobile network.

**Cracking**: It is amongst the gravest cyber crimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.

**E-Mail Spoofing**: A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it’s origin to be different from which actually it originates.

**SMS Spoofing**: Spoofing is a blocking through spam which means the unwanted uninvited messages. Here a offender steals identity of another in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of

the victim. It is very serious cyber crime against any individual.

**Carding:** It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim’s bank account malafidely. There is always unauthorized use of ATM cards in this type of cyber crimes.

**Cheating & Fraud:** It means the person who is doing the act of cyber crime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.

**Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children.

**Assault by Threat:** refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

2.4.1(B). **CRIMES AGAINST PERSON’S PROPERTY**:

As there is rapid growth in the international trade where businesses and consumers are increasingly using computers to create, transmit and to store information in the electronic form instead of traditional paper documents. There are certain offences which affects persons property which are as follows:

**Intellectual Property Crimes:** Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.

**Cyber Squatting:** It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. For example two similar names i.e. www.yahoo.com and www.yaahoo.com.

**Cyber Vandalism:** Vandalism means deliberately destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a

---

computer, some part of a computer or a peripheral attached to the computer.

**Hacking Computer System:** Hacktivism attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity there will be loss of data as well as computer. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company.

**Transmitting Virus:** Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computerize system of the individuals.

**Cyber Trespass:** It means to access someone’s computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.

**Internet Time Thefts:** Basically, Internet time theft comes under hacking. It is the use by an un-authorized person, of the Internet hours paid for by another person. The person who gets access to someone else’s ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person’s knowledge. You can identify time theft if your Internet time has to be recharged often, despite infrequent usage.

**2.4.1(C). CYBERCRIMES AGAINST GOVERNMENT**¹⁸⁶: There are certain offences done by group of persons intending to threaten the international governments by using internet facilities. It includes:

**Cyber Terrorism:** Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.

**Cyber Warfare:** It refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political

---

motivation.

**Distribution of pirated software:** It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.

**Possession of Unauthorized Information:** It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.

2.4.1(D). CYBERCRIMES AGAINST SOCIETY AT LARGE\(^{187}\):

An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. These offences include:

**Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity.

**Cyber Trafficking:** It may be trafficking in drugs, human beings, arms weapons etc. which affects large number of persons. Trafficking in the cyberspace is also a gravest crime.

**Online Gambling:** Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.

**Financial Crimes:** This type of offence is common as there is rapid growth in the users of networking sites and phone networking where culprit will try to attack by sending bogus mails or messages through internet. Ex: Using credit cards by obtaining password illegally.

** Forgery:** It means to deceive large number of persons by sending threatening mails as online business transactions are becoming the habitual need of today’s life style.

2.4.2 OFFENCES RELATED WITH CYBER CRIMES AS PER IT ACT

Offenses related with Cyber Crimes as per Information Technology Act.

A) The civil offences stipulated by section 43 and 44 of IT Act 2000 covers\textsuperscript{188}

1) Copy or extract any data, database,
2) Unauthorized access and downloading files Introduction of virus,
3) Damage to computer system and computer network,
4) Disruption of computer system and computer network,
5) Denial authorized person to access computer,
6) Providing assistance to any person to facilitate unauthorized access to a computer and
7) Charging the service availed by a person to an authorized access to a computer.

B) The criminal offences stipulated by IT ACT, 2000

CHAPTER 11 SECTIONS 65 to 75 of the IT ACT prescribe the criminal offenses which covers\textsuperscript{189}:

1) Tampering with computer sourced documents.
2) Hacking with computer systems.
3) Electronic forgery Electronic forgery for the purpose of cheating.
4) Electronic forgery for the purpose of harming reputation.
5) Using as genuine a forged electronic record.
6) Publication of digital signature certificate for fraudulent purpose.
7) Offences and contraventions by companies
8) Unauthorized access to protected systems
9) Confiscation of computer, network etc.
10) Publication information which is obscene in electronic form
11) Misrepresentation or suppressing of material facts for obtaining license.
12) Breach or confidentiality and privacy publishing false digital signature certificate.

\textsuperscript{188} IT Act 2000 Section 43 and 44
\textsuperscript{189} ITAct2000,Chapter11,Section65toSection75
2.4.3 CYBER-CRIMES COMMONLY PERPETRATED AGAINST BANKS

Perpetrators against banks can use several kinds of cyber-crimes. The most common are:

1. Spreading Viruses and worms,
2. Trojan Horse
3. Website Compromise and Malware Propagation
4. Denial-of-Service attack & Distributed Denial of Service Attack (Dos & DDoS attacks)
5. Phishing or Vishing Attacks
6. Hacking,
7. Spamming
8. Network scanning/Probing
9. Money Laundering
10. Fiscal Fraud
11. Other Offences like carders and Internet Search Engine/Google “Hacking etc.

2.4.4 TYPES OF CYBER CRIMES AGAINST E-BANKING IN INDIA

Following cyber crimes are generally committed against electronics banking:

2.4.4(A) SPREADING VIRUSES AND WORMS

Viruses and worms are computer programs that affect the storage devices of a computer or network, which then replicate information without the knowledge of the user.

Viruses: A computer virus is a computer program that can copy itself and infect a computer without permission or knowledge of the user[190]. Note that a program does not have to perform outright damage (such as deleting or corrupting files) in order to be called a "virus". Viruses are very dangerous; they are spreading faster than they are being stopped, and many of the time the least harmful of viruses could become fatal.

Full form of **VIRUS** is as under:-

**V**- Vital

**I**- Information

**R**- Resource

**U**- Under

**S**- Siege (blocked)

Generally, there are two main categories of viruses. The first category consists of the file infectors, which attached themselves to ordinary programme files. This category of viruses can be classified further as resident and nonresident. A resident or direct action virus conceals itself someplace in the memory when an infected programme is executed initially and subsequently infects other programmes when those programmes are executed.

“Jerusalem 185 virus” is the example of this\(^{191}\). Another example of resident virus is “The Vienna Virus”.\(^{192}\) Maximum viruses are resident in category. The second category of the virus is “system or boot record infectors”. Such viruses are programmed to infect executable code on a disk which is not the ordinary files. Examples of such viruses are Brain, Stoned, Empire, Azusa etc.

**Stealth Virus:** - a stealth virus is one that hides the modifications made in the file or boot record. The only completely reliable method to avoid stealth is to boot from a medium that is known to be clean.\(^{193}\)

**Polymorphic Virus:** - It is one of the viruses that produced different copies of it so as to hide itself from the detection of the virus. The virus scanner will be unreliable, and that some instances of the virus may be able to avoid detection\(^{194}\).

**Sparse infector** a virus that infects the computers only occasionally

**Companion virus** is a virus that creates a new programme by doing modification in an existing files

**Armored virus** is a virus that uses special actions to make the copy of its code more difficult. Example is the “Whale Virus”

**Macro virus** is a virus that spread through only one type of program, usually either

\(^{191}\) Jain V.K. “Computers for Beginners” by Pustak Mahal Delhi 2006 p185

\(^{192}\) http://vienna.metblogs.com

\(^{193}\) Jain N.C. “ Cyber Crimes” Allahabad Law Agency, Delhi 2008p95

\(^{194}\) ibid p97
Microsoft Word or Microsoft

**Virus hoax** is a false warning about a computer virus. The warning arrives in an e-mail note. Such messages are planned to panic computer users. The writer emails the warning and suggested the reader to forward it to others.

**Worms**: - A computer worm is a self-replicating computer program. It uses a network to spread functional copies of itself to other computer systems. Unlike viruses, worms do not need to attach themselves to an existing program\(^{195}\).

**Following are the World Famous Worms attacks**

**The Internet Worm – 1988**: Robert Morris accidentally released his worm on Arpanet (later known as Internet) in 1988. The worm controlled to infect and disabled all those machines by making copies of itself and thus clogging them.

**The SPAN Network Worm – 1989**: A Worm infected many VAX and VMS computers on the SPAN network in 1989. The worm as displayed "Worms against Nuclear Killers!" and named as “WANK” on the basis of the first letters of each word of the message.

**The Christmas tree Worm – 1987**: This warm was managed to disable the IBM network on Christmas day 1987.

**2.4.4(B) TROJAN HORSE**

A Trojan is a program that appears legitimate. However, once run, it moves on to locate password information or makes the system more vulnerable to future entry. Or a Trojan may simply destroy programs or data on the hard disk

**Trojan horse**: - It was describes in Greek mythology that the Trojan horse was a giant wooden horse placed on a platform with wheels was emerged as the gift left by an enemy army and seems that they have left the war in the evening and gone to their camp. The defending city army with a pleasure and pride took away the wooden structure on wheels inside the city covered by walls. That proved to be a grave mistake. The gigantic structure was hallow and was full of the best solders of the enemy. At the late night the solders inside the hallow structure came out quietly and laid waste to the city. The task made easy by the defending solders as they passed out earlier in the evening and celebrate the event by eating & drinking\(^{196}\)

\(^{195}\) *Ibid p103*  
\(^{196}\) *Jain N.C “Cyber Crimes” Allahabad Law Agency, Delhi 2008*p107*
A Trojan Horse is full of as much trickery as the mythological Trojan horse it was named after. The Trojan horse, at first glance will appear to be useful software but will actually do damage once installed or run on your computer. Those on the receiving end of a Trojan horse are usually tricked into opening them because they appear to be receiving legitimate software or files from a legitimate source. When a Trojan is activated on your computer, the results can vary. Some Trojans are designed to be more annoying than malicious (like changing your desktop adding silly active desktop icons) or they can cause serious damage by deleting files and destroying information on your system. Trojans are also known to create a backdoor on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.

**Types Of Trojan Horse Payloads**
The Trojan horse payloads are divided into six categories based on the capacity to break and damage the computers as under:-

i) Remote Access  
ii) Data Destruction  
iii) Downloader  
iv) Server Trojan(Proxy, FTP,IRC, Email, HTTP/HTTPS, etc)  
v) Security software disabler  
vii) Denial-of- Service attack(DoS)

**Following are the examples of damages**

a) Erasing or overwriting data on a computer  
b) Corrupting files in a subtle way  
c) Upload and download files.  
d) Allowing remote access to the victim's computer. This is called a RAT(Remote Access Trojan)  
e) Spreading other malware, such as viruses. Such types of Trojan horse are called a “dropper” or “vector”.  
f) Spying on the user of a computer and covertly reporting data like browsing habits to other people

---

g) Logging key strokes to steal information such as passwords and credit card numbers.
h) Phishing for bank or other account details, which can be used for criminal activities
i) Installing a backdoor on computer system
j) Opening and closing CD-ROM tray
k) Harvesting e-mail addresses and using them for spam.
l) Restarting the computer whenever the infected programme is started
m) Deactivating or interfering with anti-virus and firewall program
n) Deactivating or interfering with other competing forms of malware,
o) Randomly shutting off the computer.

2.4.4(C) WEBSITE COMPROMISE AND MALWARE PROPAGATION

Using fear tactics, some cyber criminals compel users to download certain software. While such software is usually presented as antivirus software, after some time these programs start attacking the user’s system. The user then has to pay the criminals to remove such viruses.

'Malware' is a general term used to refer to a variety of forms of aggressive or disturbing software. It is designed to infiltrate or damage a computer system without the consent of the owner and without his knowledge. Malware or malicious software is software used to disorder computer operation, collect important information, or get entrance to private computer systems. Malware appear in any form like code, scripts, and in the form of other software. Different types of malware are computer viruses, ransom ware, worms, trojan horses, root kits, key loggers, dialers, spyware, adware, malicious BHOs (Browser Helper Object), rogue security software and other malicious programs. Rogue security software is a Fraud Tool that deceives or misleads users into paying money for fake or simulated removal of malware (so is a form of ransom ware) or it claims to get rid of, but instead introduces malware to the computer. Rogue security software has become a growing and serious security threat in desktop computing in recent years (from 2008 on). The majority of active malware threats are usually worms or Trojans rather than viruses.

Malware is not alike the defective software. However, some malwares are masked as genuine software, and at times these malwares come from the website of the company in

---

198 Jain N.C” Cyber Crimes” Allahabad Law Agency, Delhi 2008p86
the form of a useful program along with additional tracking software that gathers marketing statistics imbedded in it. Antivirus, anti-malware, and firewalls are some of the softwares which are used at home as well as in the different organizations around the world to protect the computer system from malware attacks. These anti attack software helps in recognizing and preventing the further spread of malware in the network. Malware is often used against individuals to gain personal information such as social security numbers, bank or credit card numbers, and so on.

Types of Malwares

The Most common types of malware are as under:

1. Adware,
2. Bots,
3. Bugs,
4. Ransomware
5. Rootkits,
6. Spyware,

- **Adware:** It is a type of software supported by advertising software which automatically transports advertisement. These software repeatedly displayed on the net and attract the user by offering “free” versions that enter in the system attached with adware. Adware is generally sponsored by advertisers intend to use as revenue generating tool. Some types of adware are also spyware and can be classified as privacy invasive software.

- **BOT:** Bots are software programs produced to perform the desired operations on the computer system automatically. Video games, Internet auctions, online contests etc are some bots which are created for relatively harmless purposes. But these bots are generally used maliciously to disorder and create defect in the computers. Bots are generally used in bonnets for DDoS (Distributed Denial of Service) attacks. Bots are also used as spambot. Spam bots usually create fake accounts and send spam using them, although in many cases it would be obvious that a spambot is sending it. This has lead to the development of password-cracking spambot that are able to send spam using

---

other people's accounts\textsuperscript{202}.

- **BUG** :- Bug is a software and it creates a fault in a computer program which produces an inaccurate or surprising result. Also the software compelled it to function inadvertently.\textsuperscript{203} Minor bugs affect a program’s slightly and it takes a lot of time for its detection. Major bugs’ crash or freeze the computer system. Security bugs are the type of bugs and which can allow assailant to access and steal data.

  - **RANSOMWARE**: - Ransomware is a type of malware which restricts access to the computer system. The malware restricts user access to the computer either by encrypting files on the hard drive or locking down the system and displaying messages that are intended to force the user to pay the ransom amount to the creator of the malware creator to remove the restrictions and regain access to their computer\textsuperscript{204}.

  - **ROOTKIT**: - It is a tricky type of malicious software. The software is designed in such a way to hide the existence of certain method or programs from normal methods of detection and allowed access to a computer on the continuous basis\textsuperscript{205}. By installation of Rootkit the malicious party behind the rootkit remotely executes files, access/steal information, modify system configurations, alter software, install concealed malware, or control the computer as part of a botnet. Prevention, detection, and removal of Rootkit is not so easy because of their stealthy function. Usual security products are not effective in detecting and removing root kits. The root kits can be removed by manual methods such as monitoring computer behavior for various irregular activities. The consumers can protect their computer systems from root kits attacks by updating anti-virus on the regular basis & avoiding suspicious downloads.

  - **SPY WARE**:-Spyware is a type of software that is installed secretly on a personal computer to seize or take partial control over the computer of the user without his consent & knowledge\textsuperscript{206}. It is a type of malware that functions by spying on user

\textsuperscript{202} http://en.wikipedia.org/wiki/Spambot
\textsuperscript{203} http://en.wikipedia.org/wiki/Software_bug
\textsuperscript{204} http://en.wikipedia.org/wiki/Ransomware(malware)
\textsuperscript{205} http://en.wikipedia.org/wiki/Rootkit
\textsuperscript{206} Jain N.C. “ Cyber Crimes” Allahabad Law Agency, Delhi 2008p132
activity without their knowledge. These spying capabilities can include activity monitoring, collecting keystrokes, data harvesting (account information, logins, financial data), and more. Spyware has a capability to modify security settings of software or browsers to snooping with network connections.

2.4.4(D) DENIAL-OF-SERVICE ATTACK (DoS ATTACK) & DISTRIBUTED DENIAL-OF-SERVICE ATTACK (DDoS ATTACK)

The offences related to Denial of Service attacks and Distributed Denial of Service attacks are the examples of Website compromise. Compromised (stolen or hacked) websites continue to be an attractive target for cybercriminals who benefit primarily from the misuse of reputable domains. Cybercriminals are also able to make use of resources like processing power, bandwidth and the hosting available via compromised web servers. In order to better understand the compromise process, illicit usage, and recovery of hacked websites,

A) DENIAL-OF-SERVICE ATTACK (DoS ATTACK)

A Denial-of-Service attack (DoS attack) or Distributed Denial-of-Service attack (DDoS attack) is an attempt to deprive of to use a machine or network resource to its proposed users. DoS attack may differ in the way and means to carry out, motives for carry out and target population. DoS attack generally consists of efforts to interrupt or suspend services of a host connected to the Internet on a temporary basis or for an indefinite time period. Banks, credit card payment gateways and root name servers are always on the target of perpetrators of DoS attacks who typically target sites or services hosted on high-profile web servers as stated above.

SYMPTOMS AND MANIFESTATIONSS

The United States Computer Emergency Readiness Team (US-CERT) defines symptoms of denial-of-service attacks to include:

1) Unusually slow network performance (opening files or accessing web sites)
2) Unavailability of a particular web site
3) Inability to access any web site
4) Dramatic increase in the number of spam emails received—(this type of DoS attack is considered an e-mail bomb)

5) Disconnection of a wireless or wired internet connection

Methods of Attack

There is two general forms of DoS attacks:

1) Those attacks that crash services and
2) Those attacks that flood services.

The five basic types of DoS attack are:

1) Consumption of computational resources, such as bandwidth, disk space, or processor time.
2) Disruption of configuration information, such as routing information.
3) Disruption of state information, such as unsolicited resetting of TCP sessions.
4) Disruption of physical network components.
5) Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

B) DISTRIBUTED DENIAL-OF-SERVICE ATTACK (DDoS ATTACKS)\(^{208}\)

A distributed denial-of-service (DDoS) attack is an attack vide which a large number of compromised computer systems attack a single targeted object in this manner to cause denial of services for users of the targeted computer system. The flood of incoming messages compelled target computer system to shut down and in this way forced to deny service to the system to lawful & valid users. In a typical DDoS attack, the attacker start on by taking advantage of a weakness in one computer system and take the control of such machines and instructs to carry on the DDoS attack. The attack master, also known as the bot master, identifies the vulnerabilities in one computer and infects other vulnerable systems with malware. Ultimately, the attacker instructs the controlled machines to open an attack against another specified target.

There are two types of DDoS attacks:

1) A network- centric attack which overloads a service by using up bandwidth
2) An application-layer attack which overloads a service or database with application calls.

A computer under the control of an intruder is known as a zombie or bot A group of co-opted computers is known as a botnet or a zombie army. Both Kaspersky Labs and

\(^{208}\) http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack
Symantec have identified botnets -- not spam, viruses, or worms -- as the biggest threat to Internet security.

**Why it is called a distributed denial-of-service (DDoS) attack?**

In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a website or send spam to particular email addresses. The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the denial-of-service attack.

**How do you know if an attack is happening?**

The following symptoms indicates a DoS or DDoS attack:

- unusually slow network performance (opening files or accessing websites)
- unavailability of a particular website
- inability to access any website
- dramatic increase in the amount of spam you receive in your account

**2.4.4(E) PHISHING/ VHISHING ATTACKS**

Phishing attacks are designed to steal a person's login and password. For instance, the phishers can access the victims' bank accounts or assume control of their social network.

"Phishing" is the act of attempting to fraudulently acquire sensitive information, such as passwords and credit card details, by hidden as a trustworthy person or business with a real need for such information in seemingly official electronic notification or message.

Phishing is derived from the word fishing. Phishing is a term used for the fraud committed against bank where phishers send fake email to a random database to deceive the recipient in to divulging personal information like credit cards details, usernames and passwords that can be used for identity theft. In this era of Internet banking, phishing is one of the contemporary and fastest growing crimes on the Internet today. In the classic phishing scams, involves an e-mail that appears as came from reputable and known service institutions. By going through the e-mail it appears to be legitimate and the actual one.

---


210 Ibid

211 Jain N.C. “Cyber Crimes” Allahabad Law Agency, Delhi 2008p68
message generally specify that, due to problems in the bank such as database updates, problem occurred in server, security/identity theft concerns, the recipient is required to update personal data such as passwords, bank account information, driver's license numbers, social security numbers, Personal Identification Numbers (PIN), etc. etc. There is a open warning to the user that failure to immediately provide the updated information will result in suspension or termination of the account etc. Some of definitions are listed in the following

**Vishing or Vhishing**²¹²

Vishing, a relatively new scam, is short for voice phishing. Perpetrators of fraudulent scams use Voice over Internet Protocol (VoIP) phones to steal personal information. A con artist sends a blast e-mail, carefully disguised to appear as though it’s been sent from a financial institution, on-line payment service, or other business. It may even be so well crafted that it displays a company logo. Usually there is a report of a “security” problem and a request to call a telephone number to “straighten things out.” When victims of this crime call the telephone number (local number), they may reach an automated voice prompting them to enter account numbers, passwords, and other personal information for “verification.” In either case, because people are used to entering credit card numbers over the phone, this technique can be effective. Voice over IP (VoIP) is used for vishing because caller IDs can be spoofed and the entire operation can be brought up and taken down in a short time, compared to a real telephone line

**What component to be verified in an email to classify it as “phishing e-mail”**²¹³

Followings are the essential elements to be verified in a phishing email

1. **Generic greeting.** - Phishing e-mails are received in large batches. To save time, Internet criminals use generic names like "First Generic Bank Customer" so they don't have to type all recipients' names out and send emails one-by-one. If you don't see your name, be suspicious.

2. **Forged link:** - If there is a link in the e-mail and you recognised it doesn't to be presumed that it came from the real organization or bank. Roll your mouse over the link and see if it matches what appears in the email. If there is not matching with the original, don't click on

²¹² [http://www.pcmag.com/encyclopedia/term/57067/vishing](http://www.pcmag.com/encyclopedia/term/57067/vishing)
the link. Please note that websites where it is safe to enter personal information begin with "https" — the "s" stands for secure. If you don't see "https" do not proceed.

3. Requests personal information: - If you receive an email requesting your personal information, it is probably a phishing attempt. The reasons for sending phishing email to you in such a manner to trick you into providing your personal information.

4. Sense of urgency: - The phishers want you to provide your personal information instantly. They compel you to think something has happened with your account that requires you to send the information fast. The motive to get the information faster is to move faster on to another victim.

5. IP Address: - If URL contains an IP address, such as 12.30.229.107, instead of a domain name, you can almost be sure someone is trying to phish for your personal information.

Major factors for increase in Phishing Attacks in India:

Awareness among public: - There is a lack of awareness among the internet users particularly in India. The users are not aware that their personal information is required by criminals and do not take proper precautions while conducting online activities.

Unawareness of policy – The victims are totally unaware about their banks policies and procedures for contacting customers, particularly for issues relating to account maintenance and fraud investigation and the phishers often used victim’s unawareness on this count. Customers unaware of the policies of an online transaction became more prone to the social engineering aspect of a phishing attacks

Types of Phishing Attacks

Deceptive Phishing. The most common broadcast method today is a deceptive email message vide which the fraudsters send the e-mail that there is an urgent need to verify account information on the ground of system failure required users to re-enter their information, with the target that the victim will respond by clicking a link to or signing onto a bogus site where their confidential information can be capture

Malware-Based Phishing:-The e-mail is attached with the malware and downloadable from a culprit’s site.

Key loggers and Screen loggers phishing attack: - This type of phishing attack are the sending of malware through e-mails that track keyboard input and send relevant information

http://www.nigerianspam.com/Phishing-Types.html
to the hacker via the Internet. These malwares run automatically when the browser is started.

**Session hijacking phishing attacks**: is an attack via which users' activities are monitored. As soon as the user sign in to his account and confirms his bona fide identification the software of the perpetrator takes over the charge of the session and can start transferring funds, without the knowledge of the victim.

**Web Trojans phishing attack**: - Explode up indiscernibly when users are attempting to register in. They collect the user's credentials land transmit it to the perpetrator.

**Hosts File Poisoning**. When the user visits a website and when he types a URL, it automatically translated it in to an IP address before it transmitted over the Internet. By "poisoning" the hosts file, the wrongdoers have a bogus address transmitted, taking the user without knowing to a fake "mirror image" website where their information can be captured unlawfully.

**System Reconfiguration Attacks**: - Alter settings on a user's PC for hateful purpose. For example: URLs in a favorites file might be customized to through users to look similar websites. For example: a bank website URL may be changed from "bankofabc.com" to "bancofabc.com".

**DNS-Based Phishing ("Pharming")**: - With a pharming scheme, hackers obstruct with a company's host's so that requirements for URLs return a bogus address and subsequent communications are directed to a bogus site. Victims of such attacks are ignorant that the website where they are incoming secret information is controlled by hackers and probably not the legitimate website.

**Content-Injection Phishing**: - This type of attack illustrates the circumstances where the culprit swap part of the content of a legitimate site with false content planned to give the wrong impression about or misdirect the user into giving up their confidential information to the hacker.

**Man-in-the-Middle Phishing** is difficult to differentiate than many other forms of phishing. In these attack hacker’s location themselves between the user and the legitimate website or system

**Search Engine Phishing** occurs when phishers create websites with attractive offers and have them published legitimately with search engines. Users find the sites in the normal
course of searching for products or services and are fooled into giving up their information

**Modus Operandi of phishing attack to dupe bank customers in India:**

Recently there has been a sudden rise in the number of phishing cases in India. The most common form of phishing in India is the email pretending to be sent by a bank, where the offender asks victims to confirm their personal information/login detail for some fictional reason like bank is going to upgrade information in the server etc. The email is attached with a link of bogus website that looks exactly like the genuine site. The innocent customers thinking that the mail is received from the bank, therefore under misunderstanding he enters the information asked for and sends it into the hands of identity thieves.

The similar modus operandi was adopted by the attackers in the phishing attacks over ICICI Bank, UTI Bank, HDFC Bank, SBI etc. It was gathered that a large number of customers of these banks were sent the emails by the culprits, which appeared that these mails have been originated from their bank and sent to the customers. The customers to whom these mails were sent were instructed to update their bank account information on false pretext which was appeared to be genuine. These emails had an attachment of a hyperlink and a click to that link took recipients to a web page, which was identical to their bank’s web page. Many of the recipients of the mail responded to these mails and gave their login information and passwords. Later on, they came to know that through internet banking and by using the information rendered by them a large number of illegal/fraudulent transactions took place and also the huge amount was misappropriated.

**2.4.4( F) HACKING**

**Hacking:** The term “hacking” is used to describe the unlawful access of a computer system. It is one of the oldest computer-related crimes and in recent years has become a mass phenomenon. By targeting computer systems that host large databases, offenders can obtain identity-related data on a large scale, and this is an increasingly popular approach. In the largest case detected in the past in the USA, the thieves obtained more than 40,000,000 credit card records. Apart from direct financial profit, offenders can use identity-related information for other purposes, including using a victim’s bank account to launder money. In addition, they can circumvent identification and terrorist prevention measures by using obtained identities. The Report of the Secretary-General of the United Nations on
Recommendations for a global counter-terrorism strategy highlights the importance of developing tools to tackle identity theft in the fight against terrorism.215

**Following are the hacking tricks divided into different categories**

1) Trojan programs that share files via instant messenger
2) Phishing
3) Fake Websites.
4) Spoofing
5) Spyware
6) Electronic Bulletin Boards
7) Information Brokers/Carders
8) Internet Public Records
9) Trojan Horses
10) Identity Theft

**The Modus Operandi in Hacking Attacks**

The Modus Operandi is similar to the banking phishing attack. The spam message invites users to attend the final game of World Cup 2011 in Mumbai, India. The invite offers multiple executive club facilities such as a private table, a gourmet champagne brunch, and much more for 10 guests. This may sound like an attractive deal; however, it is simply bait for Internet users/cricket fans that are keen to be a part of the World Cup Final and experience the thrill. The Users were asked for credit card details to book tickets and packages along with their personal information which once submitted would be used to compromise the online banking account of the victim leading to financial losses to the victim

**2.4.4(G) 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 **Electronic Spamming** is the use of electronic messaging systems to send unsolicited bulk messages (spam), especially advertising, indiscriminately. While the most widely recognized form of spam is e-mail spam is the term is applied to similar abuses in other media, instant messaging spam.216,

---

How the spam-mails are used by cyber criminals against e-banking?

Consumers should be on the alert for official-looking emails that are actually spam mail sent by sophisticated identity thieves trying to trick you out of personal information that can be used to drain your bank account, fraudulently get credit cards and commit other crimes.

Fake Linked-in spam can steal your bank passwords

Linked-In spam is nothing new but this attack was particularly nasty, because it can embed password-stealing malware into your browser without you realizing it.

How the spam is related to cyber crime?

Spam can be used to spread computer virus, Trojan horse or other malicious software. The objective may be identity theft identity, or worse (e.g., advance fee fraud). Some spam attempts to capitalize on human greed whilst other attempts to use the victims’ inexperience with computer technology to trick them (e.g., phishing).

2.4.4(H) 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.

Network Attack occurs when an attacker or hacker uses certain methods or technologies to maliciously attempt to compromise the security of a network. Hackers attack corporate networks to use data for financial gain or for industrial espionage, to illegally use user accounts and privileges, to run code to damage and corrupt data, to steal data and software, to prevent legitimate authorized users from accessing network services, and for a number of other reasons.

Types of Network Attacks

1) External attacks are performed by individuals who are external to the target network or organization. External threats are usually performed by using a predefined plan and the skills of the attacker(s). One of the main characteristics of external threats is that they usually involve scanning and gathering information.

2) Internal threats originate from dissatisfied or unhappy internal employees or contractors. Internal attackers have some form of access to the system and usually try to hide their

218 http://oag.ca.gov/consumers/general/spam_phishing
219 http://searchmidmarketsecurity.techtarget.com/definition/network-scanning Posted by: Margaret Rouse
attack as a normal process.

2.4.4(i) MONEY LAUNDERING\textsuperscript{220}.

Use of banking to hold back detection of “black” money so it can be used as a legal trade tool, casually utilized by the organized crime.

**What is Money Laundering**

Money laundering 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.

**Money Laundering Steps**\textsuperscript{221}

Money laundering is generally occurred in three steps:

1. **Placement:** The first step involves introducing cash into the financial system by some means.

2. **Layering:** The second involves carrying out complex financial transactions to camouflage/con-seal the illegal source.

3. **Integration:** The final step entails acquiring wealth generated from the transactions of the illicit funds.

Some of these steps may be omitted, depending on the circumstances; for example, non-cash proceeds that are already in the financial system would have no need for placement.

**Methods of Money Laundering**\textsuperscript{222}

Money laundering can be categorized into several methods. These includes:

- **Structuring Method** also known as **Smurfing Method**
  
  This is a method of placement whereby cash is broken into smaller deposits of money, used to defeat suspicion of money laundering and to avoid anti-money laundering reporting requirements. A sub-component of this is to use smaller amounts of cash to purchase bearer instruments, such as money orders, and then ultimately deposit those, again in small amounts.

- **Bulk Cash Smuggling Method:** This involves physically smuggling cash to another

\textsuperscript{220} [http://en.wikipedia.org/wiki/Money_laundering](http://en.wikipedia.org/wiki/Money_laundering)
\textsuperscript{221} Wikipedia, the free encyclopedia
\textsuperscript{222} Ibid
jurisdiction and depositing it in a financial institution, such as an offshore bank, with greater bank secrecy or less rigorous money laundering enforcement.

**Cash-intensive businesses Method:** In this method, a business typically involved in receiving cash uses its accounts to deposit both legitimate and criminally derived cash, claiming all of it as legitimate earnings. Service businesses are best suited to this method, as such businesses have no variable costs, and it is hard to detect discrepancies between revenues and costs.

**Trade-based laundering Method:** This involves under- or overvaluing invoices to mask the movement of money.

**Shell companies and Trusts:** Trusts and shell companies (A non-trading company used as a vehicle for various financial manipulations or kept dormant for future use in some other capacity) cover up the true owner of money. Trusts and corporate vehicles, depending on the jurisdiction, need not disclose their true, beneficial, owner.

**Round-tripping Method:** Here, money is deposited in a controlled foreign corporation offshore, preferably in a tax haven where minimal records are kept, and then shipped back as a foreign direct investment, exempt from taxation. A variant on this is to transfer money to a law firm or similar organization as funds on account of fees, then to cancel the retainer and, when the money is remitted, represent the sums received from the lawyers as a legacy under a will or proceeds of litigation.

**Bank Capture Method:** In this case, money launderers or criminals buy a controlling interest in a bank, preferably in a jurisdiction with weak money laundering controls, and then move money through the bank without scrutiny.

**Casinos:** In this method, an individual walks into a casino with cash and buys chips, plays for a while, and then cashes in the chips, taking payment in a check, or just getting a receipt, claiming it as gambling winnings.

**Other gambling:** Money is spent on gambling, preferably on higher odds. The wins are shown if the source for money is asked for, while the losses are hidden.

**Real estate:** Someone purchases real estate with illegal proceeds and then sells the property. To outsiders, the proceeds from the sale look like legitimate income. Alternatively, the price of the property is manipulated: the seller agrees to a contract that under represents the value of the property, and receives criminal proceeds to make up the
difference.

**Black salaries:** A company may have unregistered employees without a written contract and pay them cash salaries. Black cash might be used to pay them.

Tax amnesties: For example, those that legalize unreported assets in tax havens and cash

**Fictional loans:** - To avail the loans from the banks and dirty money is used for repayment.

**Dirty money for private consumption:** - A goal of money laundering is to be able to use the dirty money for private consumption. If unable to use it openly, the traditional way to keep the dirty money near is hiding it as cash at home or other places. A more modern method is a credit card connected to a tax haven bank.

**Internet Banking and Money Laundering**

One of the major concerns associated with Internet Banking has been that the Internet banking transactions may become untraceable and are incredibly mobile and may easily be anonymous and may not leave a traditional audit trail by allowing instantaneous transfer of funds. It is pertinent to note that money-laundering transactions are cash transactions leaving no paper trail. Such an apprehension will be more in the case of use of electronic money or e-cash. In the case of Internet Banking the transactions are initiated and concluded between designated accounts. Further Section 11 of the proposed Prevention of Money Laundering Bill, 1999 imposes an obligation on every Banking Company, Financial Institution and intermediary to maintain a record of all the transactions or series of transactions taking place within a month, the nature and value of which may be prescribed by the Central Government. These records are to be maintained for a period of five years from the date of cessation of the transaction between the client and the banking company or the financial institution or the intermediary. This would apply to banks offering physical or Internet banking services. This will adequately guard against any misuse of the Internet banking services for the purpose of money laundering. Further the requirement of the banking companies to preserve specified ledgers, registers and other records for a period of 5 to 8 years, as per the Banking Companies (Period of Preservation of Records) Rules, 1985 promulgated by the Central Government also adequately takes care of this concern.

---

223 rbidocs.rbi.org.in/rdocs/Publication Report/
2.4.4(J) FISCAL FRAUD:
By targeting official online payment channels, cyber attackers can hamper processes such as tax collection or make fraudulent claims for benefits.

Definition of Fraud\(^{224}\)
Fraud, under Section 17 of the Indian Contract Act, 1872, includes any of the following acts committed by a party to a contract, or with his connivance, or by his agents, with intent to deceive another party thereto or his agent, or to induce him to enter into the contract:

Fiscal Fraud: - Internet banking fraud is a fraud or theft committed using online technology to illegally remove money out of one’s account. Internet banking fraud is a form of identity theft and is usually made possible through techniques such as Phishing. Other internet banking frauds are credit card withdrawal, money transaction fraud, bank account fraud, ATM fraud etc.

Definition of Cyber Fraud:
RBI had, *per se*, not defined the term ‘fraud’ in its guidelines on Frauds. No definition of “cyber fraud” is specified in Information Technology Act 2000. Instead of cyber fraud, computer fraud is defined by D. Bainbridge as ‘stealing money or property by means of a computer that is using a computer to obtain dishonestly, property including money and cheques, credit card services, or to evade dishonestly some debt or liability”\(^{225}\). Another definition of “cyber fraud” is given by The Audit Commission of the United Kingdom (UK) as “any fraudulent behaviour connected with computerization by which some one intends to gain financial advantage”\(^{226}\).

Definition of RBI Working Group on Information Security :- A definition of fraud was, however, suggested in the context of electronic banking in the Report of RBI Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, which reads as under:-

‘A *deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer*

\(^{224}\)Section 17 in The Indian Contract Act, 1872
\(^{226}\) The Audit Commission of the UK since 1987-90 study report, Para 7
system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank’.227

Therefore cyber-fraud can be termed as online theft of credit card number, expiration date, and other information for criminal gain and to cause unlawful loss to the victim which is barred by the Criminal Law of the land and for which State enforced the punishment.

ATM -FRAUDS
An automated teller machine popularly known as ATM was first introduced in 1960 by City Bank of New York on a trial basis. The main reason behind the introduction of this machine was for payment of utility bills of customers and gets a receipt without a teller. ATM allows banks and financial institutions to provide the services to their clientele with a comfortable way by 24X7 to carry out banking transactions including withdrawal of funds, made deposits, check account balance, to allow customers pay bills, etc. Authentication methods for ATM cards have been changed little bit at present as compared to applicable at the time of their introduction in the 1960’s. The means for verification of the user is the card holder’s Personal Identification Number (PIN). The intruders can discover the user’s PIN with brute force attack. The security measures were used in the ATM cards are magnetic media and the data in the magnetic stripe is usually coded using two or three tracks. F/2F technique is used for writing to the tracks of ATM Cards. Despite security measures, cases of ATM crimes continue to occur globally

TYPES OF ATM FRAUDS
In the recent past, it is reported that due to hacking in the electronic ATM system caused losses of crore in the banking sector itself. ATM attack affecting the ATM such as cloning of cards and hacking of PIN (Personal Information Number) has been reported increasingly.

SOME POPULAR ATM FRAUDS/ATTACKS ARE AS UNDER

I) CARD TRAPPING ATTACK228
Criminals are embracing methods to trap debit and credit cards in ATMs for retrieval later, a move believed to be motivated by better security measures designed to ensure card details are not copied at the machines. Card trapping instrument is designed in such a way to

228 yugioh.wikia.com/wiki/Continuous Trap Card
capture the data of the card by placing the equipment directly over or into the ATM card reader slot. By using this technique a card is physically captured by the trapping device inside the ATM. When the user leaves the ATM without their card, the card is repossessed by the culprits. Every time only one card is lost in each card trapping attack. To retrieve the ATM card of the victim the criminals have to withdraw the whole device. But now a day, a card trapping device can stay in the machine and after fixed time the card trapping device allows removal of trapped cards without the removal of the device. These types of card trapping devices are known as the Lebanese Loop.

II) SKIMMING ATTACK

This is the most popular type of attack while doing the ATM transaction. The personal data belonging to everyone who used it to swipe an ATM card is downloaded with the help of a machine known as skimmer. By using the technology i.e. with the help of the skimmer (a card swipe device that reads the information on ATM card) the intruders usually make the counterfeit ATM cards. Skimmer are resembled with a handy credit card scanner and are fixed firmly in close to an card reader. When removed from the ATM, the machine which is known as skimmer machine allows downloading of personal data of the card holder. A single skimmer machine can retain personal information of the card holders for more than 200 ATM cards at a time.

III) Phishing/Vishing Attack

Phishing tricks are planned to attract the user to provide their card number and PIN for their bank card. Phishing is a term used for the fraud committed against bank where phishers send fake email to a random database to deceive the recipient in to divulging personal information like credit cards details, usernames and passwords, that can be used for identity theft. Usually, culprits or a phishers used email and fraudulently represent them as a bank and play the tricks by claiming that recipient’s account information is incomplete, or that the recipient should urgently required to update his account information to prevent the account from being closed. Simultaneously the recipient is guided to click on a link and follow the directions provided. The link looks like the recipient’s banks web site but in fact it is the fraudulent link and designed by the attacker. By using the

---

230 en.wikipedia.org/wiki/SMS_phishing
phishing tricks the sensitive information such as card numbers and PINs are collected by the attackers. The information so collected by the attackers used to create fake ATM cards fraudulently. After getting success of phishing attack, the criminal would take out the needed information and remove the victim’s bank funds by login the victims account on line. Now a day’s many banks and financial institutions are now proposing check images as part of their online banking services to their customers. The checks contain the customer’s bank account number, signature, address, phone etc. Now a day’s some of the criminals has changed their style of committing the crime. In place of cheating the victim's account; they visit the check image page and wherefrom they copied the victim's check. By copying the check the attacker can either make paper counterfeit checks, or by using the information can create a PayPal accounts or other online payment accounts and hooked the victim for any damages..

**Vishing, a relatively new scam**, is short for voice phishing.²³¹Perpetrators of fraudulent scams use Voice over Internet Protocol (VoIP) phones to steal personal information. When victims of this crime call the telephone number (local number), they may reach an automated voice prompting them to enter account numbers, passwords, and other personal information for “verification.” In either case, because people are used to entering credit card numbers over the phone, this technique can be effective. Voice over IP (VoIP) is used for vishing because caller IDs can be spoofed and the entire operation can be brought up and taken down in a short time, compared to a real telephone line.

**IV) PIN CRACKING ATTACK²³²**

The customer PIN is the primary security measure against fraud; forgery of the magnetic stripe on cards is minor as compared to PIN acquisition. A criminal can without difficulty steal a ATM card, but unless he observes the customer enter the PIN at an ATM, he can only guesses to match against a possible 10,000 PINs and would be treated lucky if his guess is successful. The processing systems of ATM card used by the banks are open to abuse. Generally, an abuse functions that are used by the banks to allow customers to select their PINs online creates an opportunity an attacker to discover PIN codes. Example of such abuse functions adopted by the banks those were entered by customers while

---

²³¹ [http://www.pcmag.com/encyclopedia/term/57067/vishing](http://www.pcmag.com/encyclopedia/term/57067/vishing)
withdrawing cash from an ATM providing they have access to the online PIN verification facility or switching processes. A bank insider could use an existing Hardware Security Module (HSM) to reveal the encrypted PIN codes. The pin cracking is the insider attack and it could not be possible without the help of the insider.²³³

V) ATM HACKING²³⁴
Attackers may hack ATM’s and withdraw cash from people whose ATM information he has stole. Usually this does not result in loss of reputation since it is not something that can be witnessed. Attackers use sophisticated programming methods to crack into websites which is placed on a financial institution’s network. By accessing the website of the bank, the attackers can enter the bank’s systems to find the ATM database and by this way they collect card information. By using this information the attackers later on creates the clone of the ATM card of the victim. Hacking in addition to frequently used to depict attacks against card processors and other mechanism of the transaction processing network. Most of the ATM hackings has taken place due to the use of non-secure ATM software²³⁵.

VI) ATM PHYSICAL ATTACK²³⁶
ATM physical attacks are attempted on the safe inside the ATM, through mechanical or thermal means with the intention of breaking the safe to collect the cash inside. Some of the most common methods include ram raids, explosive attacks and cutting. Robbery can also occur when ATMs are being replenished or serviced. Staffs are either held up as they are carrying money to or from an ATM, or when the ATM safe is open and cash cassettes replaced.

VII) ATM MALWARE ATTACKS²³⁷
Malware attacks required an insider, such as an ATM technician who has a key to the machine, to place the malware on the ATM. Once that was done, the attackers could insert a control card into the machine’s card reader to trigger the malware and give them control of the machine through a custom interface and the ATM’s keypad.

²³⁴ en.wikipedia.org/wiki/Barnaby Jack
²³⁵ http://watchdogs.gamepedia.com/ATM_Hacking
²³⁶ www.diebold.com/products.../atm-self.../atm.../atm-physical-security.asp..
²³⁷ en.wikipedia.org/wiki/Barnaby Jack
2.4.4(K) OTHER OFFENCES OF CYBER CRIMES

a) 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

b) Internet Search Engine/Google “Hacking”:- One key cyber-tool used by criminals is the Internet search engine, such as Google. Credit card numbers are easily pulled and bank account numbers can be found if placed improperly on the Web. This misuse of Google is referred to as “Google hacking

2.4.4.(L) OTHER CYBER CRIMES RELATED WITH BANKING

I) Data Theft in E-Banking in India
Cyber Crimes 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.

II) Cyber Terrorism against E-Banking in India
Following are the tools of cyber terrorism against banking
(a) Hacking (b) Trojans (c) Computer Viruses (d) Computer Worms (e) E-Mail Related Crime (f) Denial of Service (g) Money Laundering (h) Terrorist financing

III) Jurisdictional Problem against E-Banking in India
Cyber crime does not know by any geographical boundaries 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

IV) Extradition of offenders Jurisdiction In case of Cyber Crime:
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

V) Evidence related problems of cyber crimes in e-banking
There are various problems faced by the banking industry related with electronic evidence. As a result of development of technology, a new variety of crime called the cyber crime has emerged which is radically different from the traditional crimes. The cyber crimes are growing day by day and the existing cyber regulations are not efficient to control the growth of such crimes. To control cyber crimes in the country there should be an effective cyber law the country.