About the Book

This is an edited book comprising selected papers submitted to the National Seminar on “Banking Services: Problems and Perspectives” organized by the Chair of Excellence on Consumer Law and Jurisprudence of the Tamil Nadu Dr.Ambedkar Law University, Chennai in association with Ministry of Consumer Affairs, Food and Public Distribution, Department of Consumer Affairs, Government of India on 23rd and 24th December, 2018. The papers have been classified under six sections as follows: (i) New trends in Banking; (ii) e-Banking and related issues; (iii) Grievance Redressal Mechanism in the Banking Sector; (iv) Banking Laws and Reforms; (v) Prevention of Frauds in Banks and (vi) Role of RBI in regulating Banks.

About the University

The Tamil Nadu Dr.Ambedkar Law University is a premier institution for legal education, established in the year 1997 in pursuance of the Tamil Nadu Act No.43 of 1997. As a sui generis model, the University is the first of its kind in the country offering legal education both on its campus and through the affiliated law colleges in the State of Tamil Nadu. All the ten Government Law Colleges and twoPrivate Law Colleges stand affiliated to the Tamil Nadu Dr.Ambedkar Law University. The University has established a School of Excellence in Law in the University Campus.

About the Chair of Excellence on Consumer Law and Jurisprudence

The Chair of Excellence on Consumer Law and Jurisprudence named after late Shri.A.K.Venkata Subramaniam, a former Secretary, Government of India and a Consumer Activist has been functioning since 01.07.2014. The objectives of the Chair, among others, are (i) to provide for the advancement and dissemination of knowledge of law and their role in the development of better education; (ii) to promote legal education and well being of the community generally and (iii) to provide access to legal education of large segments of the population and in particular to the disadvantaged groups.

ISBN 978-93-87882-83-6

Published By

Shri A.K.Venkata Subramaniam
Chair of Excellence on Consumer Law and Jurisprudence (CECLJ),
The Tamil Nadu Dr.Ambedkar Law University, Chennai.

A Project Funded By

Department of Consumer Affairs,
Ministry of Consumer Affairs, Food and Public Distribution,
Government of India.

BANKING SERVICES: PROBLEMS AND PERSPECTIVES

सत्यमेव जयते

BANKING SERVICES: PROBLEMS AND PERSPECTIVES

BANKING SERVICES:

PROBLEMS AND PERSPECTIVES

BANKING SERVICES:

PROBLEMS AND PERSPECTIVES

Papers presented at the National Seminar organized by

THE TAMIL NADU DR.AMBEDKAR LAW UNIVERSITY CHENNAI

Shri.A.K.Venkata Subramaniam
Chair of Excellence on Consumer Law and Jurisprudence

with financial support from the

Ministry of Consumer Affairs, Food and Public Distribution
(Department of Consumer Affairs), Government of India

on

23rd and 24th December, 2018.

BANKING SERVICES: PROBLEMS AND PERSPECTIVES

Patron

Prof.(Dr.) T.S.N. Sastry
Vice-Chancellor
The Tamil Nadu Dr.Ambedkar Law University,
Chennai.

Chief Editors

Thiru. R. Santhanam, Honorary Director
Dr. Ranjit Oommen Abraham, Project Director

Associate Editors

Thiru.R. Karuppasamy, Project Manager
Tmt. Deepa Manickam, Assistant Professor
Thiru.V. Anandha Kumar, Research Associate

Published By

SHRI.A.K.VENKATA SUBRAMANIAM,
CHAIR OF EXCELLENCE ON CONSUMER LAW AND JURISPRUDENCE (CECLJ),
THE TAMIL NADU DR. AMBEDKAR LAW UNIVERSITY, CHENNAI.

Funded by

MINISTRY OF CONSUMER AFFAIRS, FOOD AND PUBLIC DISTRIBUTION
(Department of Consumer Affairs), GOVT. OF INDIA.

Year of Publication : 2019

ISBN No : 978-93-87882-83-6

Typeset and Aligned by:

A. Komathi, Junior Assistant, CECLJ, TNDALU.

The Tamil Nadu Dr.Ambedkar Law University
"Poompozhil", #5, Dr.D.G.S.Dinakaran Salai, Chennai – 600 028

Prof. T.S.N. Sastry, Ph.D. (Law),,
Vice-Chancellor

22.05.2019

Foreword

The concept of consumer protection is rapidly changing in different dimensions and perspectives due to the impact of various doctrines that have evolved through legislative and judicial developments. This transformation has seen the real empowerment of consumers in many developed countries and the consumer jurisprudence started to evolve and dwell in the shadow of this doctrine. The legal and judicial understanding pertaining to the present generations of consumers also were impacted a lot and the whole world witnessed the phenomenon of consumerism sweeping in all dimensions and spheres of life. The consumer legislations and also the related laws need constant updating for the purpose of strengthening the rights and protection of consumers in the society. Globalisation and Liberalisation have literally turned the universe into a global village of goods and services and transactions leading to exchange of such services are rapidly increasing day by day. The concept and nature of consumers and consumerism has also impacted various service sectors in many aspects.

The banking services and consumer related issues started to face new challenges after the digitalisation and introduction of modern banking in India. The technological influence that changed the banking industry has also changed the manner of services that have been rendered in the present day system of banking. The various issues that have cropped up as a result to include payments without authorisation, privacy of data, grievance redressal and emergence of alternative currency. The numerous cross border transactions due to the impact of globalization have also created new challenges to the banking sector. The jurisdictional constraints and conflict of laws in different countries that have to be understood in the context of cross border transaction have underlined the need for coordination and cooperation in the international banking.

In this context the Chair of Excellence in Consumer Law and Jurisprudence (CECLJ), the Tamil Nadu Dr Ambedkar Law University, which organized a two-day National Seminar on "Banking Services-Problems and Perspectives" has taken the initiative of bringing out this edited book of selected

papers presented at the Seminar mainly for the purpose of spreading awareness among all segments of society. I'm happy that the Chair is constantly doing its best efforts to make sure that consumer consciousness is embedded into the minds and hearts of all consumers .The Chair's various activities involving publication and field research have been encouraged and appreciated by many stakeholders. I thank the Ministry of Consumer Affairs, Food and Public Distribution (Department of Consumer Affairs), Government of India for all the support and encouragement to CECLJ in its activities. I commend the participants who were involved in the contribution of various articles on many important and contemporary aspects of Banking services and technology.

(Prof. T.S.N. Sastry)

PREFACE

In the context of economic liberalisation and globalisation, various reforms in banking sectors have been introduced from time to time in India to improve the operational efficiency and promote the health and financial soundness of banks and make them achieve internationally accepted standards of performance. Internet and mobile banking, new products such as investment advisory services, cash management services, tax advisory services etc. have increased the popularity of banks. But there are a few problems that have been plaguing the banking sector in our country- the problem of non-performing assets (NPAs), the increasing number of bank frauds, the threat of cybercrimes, the perception that banks cater more .to the corporate houses and the urban elite than address the problems of the rural poor etc. In this context the role of RBI as the regulator vis-à-vis the Government's policies has also come under public scrutiny.

The Banking Regulation Act 1949, which regulates all banking firms in India, also gives RBI the power to regulate, control and inspect all Indian Banks. Does the Act need a relook in the light of the developments that have taken place in the banking sector in recent years? To what extent has the Prevention of Money Laundering Act 2002 helped in tackling this serious problem? Do the provisions of the Consumer Protection Act 1986 and the Information Technology Act 2000 have enough teeth to redress the grievances of consumers with regard to banking services? These and other issues were discussed threadbare at the two-day National Seminar on "Banking Services: Problems and Perspectives" organized by the Shri.A.K.Venkata Subramaniam Chair of Excellence on Consumer Law and Jurisprudence of the Tamil Nadu Dr.Ambedkar Law University, Chennai on 23rd and 24th December, 2018 in which academicians, bank officials, consumer related NGOs, research scholars and students participated.

Papers were invited on the following themes: (i) e-Banking and the consumer (ii) Banking services - A SWOT analysis (iii) New trends in bank-customer relationships (iv) Changing dimensions in loans and

advances (v) Money laundering as a major issue (vi) Privacy Issues in Banking Transactions (vii) Efficient ways of controlling frauds in the banking sector (viii) Non-performing assets (NPS) and ways to reduce them. (ix) Do banking laws need major reforms? (x) Issues in e-wallet (xi) Grievance redressal mechanism in banking sector and (xii) Role of RBI in regulating banks. There was excellent response and about 80 papers on the above themes were presented over two days.

Some of the papers presented at the seminar have been edited and selected for publication in this volume under the following sections:

Section-I : New trends in Banking.
Section-II : e-Banking and related issues.
Section-III : Grievance Redressal Mechanism in the Banking Sector.
Section-IV : Banking Laws and Reforms.
Section-V : Prevention of Frauds in Banks.
Section-VI : Role of RBI in Regulating Banks.

We thank Prof. (Dr).T.S.N. Sastry, Vice-Chancellor of the University for his guidance and support in organising the seminar and bringing out the publication.

The editors record their deep sense of gratitude to the Hon'ble Thiru Justice V.Ramasubramanian, Judge, Andhra Pradesh & Telengana High Court for his insightful inaugural address at the seminar and to Prof.(Dr).A.Rajendra Prasad, former Vice Chancellor, Acharya Nagarjuna University, Guntur, Andhra Pradesh for his thought provoking valedictory address. The Editors wish to thank the contributors of the papers for their enthusiastic response. The views expressed in the papers are of the respective authors only. The Editors are no way responsible for the authenticity of facts or the contents of the articles. We hope the readers will find this publication useful and relevant.

Chennai
21.05.2019. **Editors**

Theme and sub-themes of the Seminar

Sections	Theme and sub-themes
I	**New trends in Banking** Sub-themes covered: 1. New trends in Banks – Customer relationship. 2. Changing dimensions in Loans and Advances.
II	**E-Banking and related issues** Sub-themes covered: 1. e-Banking and the Consumer. 2. Issues in e-wallet.
III	**Grievance Redressal Mechanism in the Banking Sector** Sub-themes covered: 1. Grievance Redressal Mechanism in the Banking Sector. 2. Privacy issues in Banking transactions.
IV	**Banking Laws and Reforms** Sub-themes covered: 1. Do Banking Laws need major reforms? 2. Non-performing assets and ways to reduce them.
V	**Prevention of Frauds in Banks** Sub-themes covered: 1. Efficient ways of controlling Frauds in Banking sector. 2. Money Laundering as a major issue.
VI	**Role of RBI in regulating Banks** Sub-themes covered: 1. Banking Services – A SWOT analysis. 2. Role of RBI in regulating Banks.

CONTENTS

Section-I

New trends in Banking

"FROM LENDERS' HAIRCUT AND SACRIFICES TO LOAN WAIVERS – LAW AND PRACTICES IN INDIA"

M. SIVARAMAN*
&
S. JEEVITHA**

ABSTRACT:

Banks and lenders have always enjoyed discretion to either postpone and/or scale down their recoveries of bad loan accounts. When the loan repayments hit roadblocks arising out of genuine circumstances, lenders have often permitted moratorium against recovery and even took haircuts and sacrifices on their principal and interest receivables with a view to reviving and rehabilitating the lenders. Traditionally, under the voluntary route the lenders have acted through the non-statutory mechanisms such as One Time Settlement, Roll Over, Corporate Debt Restructuring, Strategic Debt Restructuring and Sustainable Structuring of Stressed Assets schemes, until February 2018 when the Reserve Bank of India abolished such restructuring schemes. Involuntarily, the banks were also, from time to time, enjoined by popular governments to enforce crop loan and cooperative loan waivers. In terms of statutorily recognized schemes envisaged by the Sick Industrial Companies Act, Insolvency legislations and the SARFAESI Act, the lenders are permitted to take haircuts and make sacrifices in the loan recovery. In recent times, under the Insolvency and Bankruptcy Code, the financial creditors end up making huge sacrifices of the loans owed by corporate entities which are admitted into Corporate Insolvency Resolution Process.

This paper critically examines the legal and regulatory challenges associated with such loan waivers, sacrifices and haircuts. The relevant international practices on this subject and the judicial pronouncements on this subject will also be discussed.

* Ph.D Scholar, The Tamil Nadu Dr. Ambedkar Law University, Chennai.
** II year B.A., LL.B (Hons), VIT School of Law, Chennai.

General Obligations of Lenders towards Borrowers:

Once loan application is received and sanctioned for the borrower, if the lender delays or refuses to actually disburse the loan sanctioned, it can be compelled for specific performance of the contract even through a writ court[1] and banks may also end up in paying damages and specific performance to release the sanctioned loan[2]. Timely release of sanctioned loans is also one of their paramount obligations[3]. Proper and correct statements of the loan accounts should be rendered by the banks towards the borrowers[4]. Banks are to extend fair, reasonable and non-discriminatory treatment to their borrowers[5]. Excessive interest charging by lenders in violation of the Fair Practices Code[6] cannot be condoned or ignored by the Reserve Bank of India ("RBI") and in any case they cannot charge interests over interests[7]. Re-scheduling or offering rehabilitation package to the borrowers has now become well recognized and entrenched in our fiscal policy and law. Banks and lenders cannot pursue plural remedies against their borrowers[8]. They are under a duty to respond to the representations received from the borrowers[9]. They can also be fastened by the borrowers with counter-claims[10]. Any action taken by lenders for attachment and sale of the secured assets cannot extinguish the right of redemption vested with the borrowers[11] which could remain open until sale is completed through registration[12]. Even then, a borrower may still challenge the auction sale on the basis that it did not fetch the best possible deal *vis-à-vis* the one offered for settlement by the borrower[13]. They should ensure that best possible price is realized for

[1] *Gujarat State Finance Corporation v. M/s. Lotus Hotels Pvt. Ltd.* AIR 1983 SC 848
[2] *Indian Bank v. ABS Marine* MANU/SC/2046/2006 : AIR2006SC1899
[3] *Mahesh Chandra v. Regional Manager, UP Financial Corporation* AIR 1993 SC 935
[4] *Central Bank of India v. Ravindra & Ors.* AIR 2001 SC 3095
[5] See *Gujarat State Finance Corporation v. M/s. Lotus Hotels Pvt. Ltd.* AIR 1983 SC 848, *Mahesh Chandra v. Regional Manager, UP Financial Corporation* AIR 1993 SC 935; *State Financial Corpn. v. M/s. Jagdamba Oil Mills* AIR 2002 SC 834;
[6] *A. R.Jeyarhuthran vs. The Union of India and Ors* legalcrystal.com/1171472 decided on November 14, 2014
[7] *Central Bank of India v. Ravindra & Ors.* AIR 2001 SC 3095
[8] *A.P. State Financial Corporation v. M/s. GAR Re-Rolling Mills* AIR 1994 SC 2151
[9] *Maharashtra State Finance Corporation v. M/s. Suvarna Board Mills* AIR 1994 SC 2657 and *Mardia Chemicals Ltd. and Ors. vs. the Union of India and Ors.* 2004 SOL Case No.298
[10] *M.E. Industries Pvt. Ltd. v. Banaras State Bank Ltd.* AIR 2000 All 181
[11] *Ganga Dhar v. Shankar Lal* : [1959] 1 SCR 509; *Maganlal v. M/s. Jaiswal Industries, Neemach* AIR 1989 SC 2113
[12] *Mathew Varghese vs. M. Amritha Kumar and Ors.* MANU/SC/0114/2014
[13] *Chairman and Managing Director, SIPCOT, Madras v. Contromix Pvt. Ltd.* AIR 1995 SC 1632

the assets of the borrowers secured with them when they are sold[14]. They cannot retain excess monies which remain with them after satisfaction of all claims due by the borrowers and ought to return the excess to the borrowers[15]. They cannot use strong-arm tactics and forcibly recover the loans[16]and may even stand to face criminal prosecution for such practices[17]. They cannot declare borrowers as 'willful defaulters' without following the due process of law[18]. They have no escape and are obliged to act on the guidelines of RBI in extending OTS in a non-discriminatory fashion, provided the borrower's case falls within the guidelines issued by RBI[19]. Banks can seek recompense only if the assets released through OTS are sold by the borrowers within three years of such settlement and there is no restriction for the borrowers in raising money by creating third party interest over such assets without selling the same[20].

The various statutory prescriptions, judicial pronouncements and practices as highlighted above have seriously constrained the ability of the banks and lenders to recover their loan receivables and have not only led to the mounting of Non-Performing Assets ("NPA"), but, have also jeopardized and eroded the capital adequacy of the banks and financial institutions in India. Some of the means and mechanisms through which banks and lenders invariably end up in NPAs and suffer capital erosion are illustrated below.

Roll-over of Loans and Ever-greening:

Roll-over of loans is a legitimate process when the lender agrees to extend the period of loan repayment of a borrower's account for bona fide business difficulties. However, ever-greening is an invidious practice adopted by some banks to sanction fresh loans so as to settle

[14] See *J. Rajiv Subramaniyan and Ors. vs. Pandiyas and Ors*. (14.03.2014 - SC) : MANU/SC/0207/2014 and *Vasu P. Shetty vs. Hotel Vandana Palace and Ors.* (22.04.2014 - SC) : MANU/SC/0341/2014

[15] See *Swastic Automobiles, M/s. v. Bihar State Financial Corporation* AIR 1989 SC 1551 and *H.P. State Financial Corpn., Shimla v. Prem Nath Nanda* AIR 2001 SC 5.

[16] *Manager, ICICI Bank Ltd.v. Prakash Kaur and Ors.*III (2007) SLT 1=138 (2007) DLT 248 (SC); *Citicorp Maruti Finance Ltd. v. S. Vijayalaxmi* reported in III (2007) CPJ 161 (NC).

[17] See *ICICI Bank vs. Shanti Devi Sharma and Ors*. legalcrystal.com/677540

[18] See *Subhiksha Trading Services Limited, Chennai, Company Secretary, M.Rathinakumar vs. Kotak Mahindra Bank Limited, and Ors.* 2009 INDLAW MAD 1694 and *Sudarshan Overseas Limited vs. Reserve Bank of India and Another* 2009 INDLAW DEL 626

[19] *Sardar Associates and Ors. vs. Punjab and Sind Bank and Ors*. (31.07.2009 - SC) : MANU/SC/1351/2009

[20] *Punjab and Sind Bank vs. Punjab Breeders Ltd. and Ors*. (29.03.2016 - SC) : MANU/SC/0366/2016

the overdue loan accounts which would otherwise slip into NPA defaults. Both these processes, however, have an effect of reduced or doubtful recovery chances which over a period of time seriously affect the lenders' ability to collect chronic loan defaults.

Moratorium on Repayments and Recovery Proceedings:

Banks have discretion to effect a moratorium on the repayments in case borrowers have genuine difficulties in servicing the loans. The repayment is merely deferred and delayed in the case of moratorium of repayment for a definite period as in the case of CDR and upon the expiry of said moratorium period, the repayment installments would commence. The loss of interests arising out of such moratorium erodes the lender's capital. Suspension of legal proceedings, including recovery of loans, as envisaged under section 22 of the Sick Industrial Companies Act, 1984 ("SICA") was greatly abused by the borrowers in our country resulting in the perpetual deferment of recovery proceedings by lenders. The successor legislation to the SICA *viz*. IBC, 2016 which introduced moratorium under section 14 of IBC is limited in duration to 180 days extendable by another 90 days which protects only the corporate debtor and is no more available to the protection of its guarantors[21]. This moratorium sometimes has the effect of not only delaying, but also defeating the recovery possibilities of the loan account causing losses to the banks.

One Time Settlement:

RBI guidelines as adopted by the individual scheduled commercial banks policies hold the field in relation to entertaining of borrower's requests for approval of OTS, mostly in relation to the Micro, Small and Medium Enterprises Sector[22]. Usually the banks seek to realise at least the outstanding principal and in most circumstances the banks forgo the interests where the borrowers have acted genuine and have not resorted to either diversion or siphoning of the funds. In this process, banks end up sacrificing the interests, costs and other charges over the outstanding loans with the haircuts taken by the banks often

[21] *State Bank of India vs. V. Ramakrishnan and Ors*. MANU/SC/0849/2018.
[22] See RBI Circular No.RBI/2008-09/467 RPCD. SME & NFS. BC.No.102/06.04.01/2008-09 dated May 4, 2009.

in the range of 40-60 per cent[23] which even extend up to 90% of the loan receivables[24]. RBI only lays down guidelines for such haircuts, but, it is the prerogative of each commercial bank to decide on the quantum of haircut it can take for its borrowers' loans[25]. In this process, the only advantage which accrues to the banks is the immediate liquidity of the principal amount whose Net Present Value is better than the uncertainties associated with recovery proceedings. OTS results in the compromise and settlement of all pending cases and the relinquishment of right to initiate any fresh cases against the borrowers.

Scheme of Arrangements:

The scheme of compromise with lenders and scheme of arrangement by companies under section 391 to 394 of the erstwhile Companies Act, 1956 was one of the most resorted practices which resulted in the restructuring of companies with huge loan recasts, deferments, moratorium and haircuts and sacrifices made by the banks and financial institutions so as to revive the companies under schemes which are approved by the High Courts.

Revival Scheme under SICA:

Most rehabilitation packages cast an obligation upon the participating banks/creditors (who might be entitled to claim outstanding dues from the sick company) to not only forego some part of the interest liabilities or even accept a lump sum settlement, but also to do something positive, i.e. to increase/enhance or continue with recurring funding of a venture which otherwise would be wound-up[26]. Under section 19 of the SICA when any scheme is sanctioned by BIFR it had required lenders to provide further financial assistance to a sick industrial company by way of loans, advances or guarantees or reliefs or concessions or sacrifices which led to the frittering away of the financial resources of the banks in our country. In the case of BIFR scheme the sick industries are given financial assistance by way of

[23] See https://www.thehindubusinessline.com/money-and-banking/banks-have-to-take-up-to-50-haircut-on-stressed-debt-of-rs-50000-cr-under-ice-framework-study/article24933342.ece as accessed on 16.11.2018

[24] See https://www.financialexpress.com/industry/banking-finance/idbi-bank-default-cases-settled-with-90-pct-haircut-malvika-steel-to-usha-ispat-see-how-surprisingly-low-settlement-was/950181/ as last accessed on 16.11.2018

[25] See https://www.thehindubusinessline.com/money-and-banking/banks-not-rbi-will-decide-size-of-badloan-haircuts/article9686869.ece as accessed on 16.11.2018

[26] *IndusInd Bank Ltd. vs ITI Limited and Ors.* decided by Delhi High Court on 11 July, 2014

loans, advances or guarantees or reliefs or concessions or sacrifices by Government, banks public financial institutions and other authorities[27].

Corporate Debt Restructuring:

CDR was introduced by RBI as a voluntary non-statutory arrangement by banks to restructure the accounts of borrowers who are not classified as willful defaulters and whose accounts do not involve any frauds. Several corporates in our country have availed CDR and some of them even availed CDR twice. The CDR cell has approved restructuring of stressed loans worth Rs.4 trillion since its inception in 2001, of which Rs.84,677 crore worth of loans exited the CDR cell successfully while Rs.1.84 trillion exited without success and now nearly Rupees 1.32 trillion worth of bad loans are presently undergoing restructuring in the cell[28]. In a typical case of CDR, the lenders agree to a moratorium, sacrifice of loan principal and interest receivables, recasting the loans, extending the repayment schedule and in some cases releasing of additional and fresh loans to help revive the borrower companies. In some CDR cases, the lenders may also agree to convert their debt into equity in the borrower company thereby reducing the quantum of loans and in return may seek a right of recompense which is very illusory. In all instances of CDR, there is a huge write-off and loss to the receivables of a bank, by way of hair-cuts and sacrifices. Courts have held that CDR package also binds the non-member banks of a borrower[29] and with a view to ensuring revival of the CDR companies they were exempted from onerous financial obligations[30] while in some instances injunction against invocation of bank guarantees were issued to help such companies[31], and even governments were directed to support the obligations undertaken to be discharged by them in terms of the CDR scheme[32]. The implementation of CDR schemes by the Indian banking sector had resulted in draining

[27] *Deputy Commercial Tax Officer and Ors. vs. Corromandal Pharmaceuticals and Ors*. MANU/SC/1598/1997

[28] See https://www.livemint.com/Industry/k2S0MIBwJ1Imv7x6PXPxSJ/RBI-moves-to-wind-up-CDR-system.html as accessed on 12.12.2018

[29] *Yes Bank Limited Vs. A2z Maintenance and Engineering Services Ltd. and Ors* Delhi High Court decision dated July 30, 2014 legalcrystal.com/1159118

[30] *IDBI Trusteeship Services Ltd. and anr Vs. Arch Pharmalabs Ltd. and ors* Delhi High Court decision dated August 24, 2014 legalcrystal.com/1162953

[31] *Geodesik Techniques Private Limited vs. Larsen and Tourbro* Madras High Court decision dated March 28, 2014 legalcrystal.com/1136543

[32] *AIDQUA Holdings Mauritius Incvs. Tamil Nadu Water Investment Co. Ltd.* Madras High Court decision January 31, 2014 legalcrystal.com/1124006

their resource pool so much that the banks are requiring re-capitalisation today.

Assignment to Asset Reconstruction Companies:

With the enactment of the SARFAESI Act, 2002, the banks and financial institutions were permitted to assign and sell their loans to Asset Reconstruction Companies ("ARC") in terms of section 5 thereof, at huge discounts. This enabled the banks and financial institutions to quickly get rid of their sticky loans and NPAs to ARCs and realise only a part of the value of the outstanding loan receivables of its borrowers. ARCs remit only a small upfront money and subsequently settle a heavily discounted consideration to the banks for such assignment and the same was neither considered to be against public policy nor the receipt of only a meagre portion of their loan receivables from the ARCs[33]struck down by our courts. Worse such assignment of loans were also attracting huge stamp duty, which now stands exempted in terms of the amendment made to section 5 of SARFAESI Act in 2016. The banks and financial institutions lost heavily on these assignments of loans, but, in the process only managed to clean-up their balance-sheets.

Loan Write-off and Waivers:

As per the RBI data on global operations, public sector banks have written off, including compromise, an amount of Rs.241,911 crores from 2014-15 till September 2017[34] which amount stood at Rs.3,16,500 crore as on April 2018[35]. Government of India has clarified that "*writing off of loans is done, inter alia, for tax benefit and capital optimization. Borrowers of such written off loans continue to be liable for repayment. Recovery of dues take place on ongoing basis under applicable legal mechanisms. Therefore, write-off does not benefit borrowers[36]*."

[33] See *ICICI Bank vs. Official Liquidator of APS Star Ltd.* AIR 2011 SC 1521

[34] See https://www.businesstoday.in/current/economy-politics/govt-has-written-off-rs-2.4-lakh-crore-bad-loans-in-three-years/story/274077.html as accessed on 12.12.2018

[35] See https://www.financialexpress.com/industry/banking-finance/explained-loan-write-off-is-not-the-same-as-loan-waiver-what-you-should-know/1335139/ as accessed on 12.12.2018

[36] The Press Release dated March 28, 2018 of the Ministry of Finance, Government of India.

On the other hand, our judiciary holds that a bank may exercise their "right of waiver" unilaterally to absolve the debtor from its liability to repay and upon such exercise, in which event the debtor is deemed to be absolved from the liability of repayment of loan subject to the conditions of waiver[37]. The last debt waiver scheme *viz*. Agricultural Debt Waiver and Debt Relief Scheme, 2008 (ADWDRS, 2008) announced by the Union Government was implemented in the year 2008, where under the debt waiver portion of the ADWDRS, 2008 was closed by its due date i.e. 30.6.2008, while the debt relief portion of the Scheme was closed on 30.6.2010, with its benefits having been extended to 3.73 crore farmers to an extent of Rs.52,259.86 crore[38]. This was followed up several state governments extending their own loan waiver schemes as part of their election manifestos which resulted in huge losses to the cooperative and rural banks, despite objections by RBI[39] and it is estimated that if every state were to waive even 50% of their agricultural debt, it would cost 1% of India's GDP in terms of 2016-17 price[40].

In the Debt Relief Scheme issued by the Government of India, when eligibility for loan waivers had not been defined exhaustively, but only a few examples were mentioned, which can be extended up to a number of other activities which have not been explicitly mentioned as the term '*etc*.' our judiciary extended relief to borrowers who were affected by militancy[41]. The Madras High Court has ruled that the denial of benefit of waiver of crop loans to the farmers who had cultivated lands exceeding 5 acres is a clear discrimination violating Article 14 of the Constitution of India and directed that the benefit of crop loan waiver scheme should be extended to farmers holding more than 5 acres as well[42]. But, this decision of the Madras High Court was eventually stayed by the Supreme Court in July 2017[43].

---

[37] *The Commissioner vs. Mahindra and Mahindra Ltd.* (24.04.2018 - SC) : MANU/SC/0513/2018

[38] The Press Release dated March 28, 2018 of the Ministry of Finance, Government of India.

[39] See https://www.orfonline.org/expert-speak/are-loan-waivers-breeding-a-defaulter-nation/ accessed on 12.12.2018

[40] NilanjanBanik, *Are Loan Waivers a Panacea for Rural Distress?*, Economic & Political Weekly, Vol. LIII No.47, December 1, 2018

[41] *Jammu Rural Bank vs. Mohd. Din and Ors*. (29.08.2008 - SC) : MANU/SC/3674/2008

[42] *National South Indian vs The Government of Tamil Nadu* Madras High Court decision dated 04.04.2017 https://indiankanoon.org/doc/61680939/

[43] See https://www.thehindu.com/news/national/tamil-nadu/sc-stays-madras-hc-order-directing-tn-govt-to-waive-all-crop-loans/article19202600.ece as accessed on 12.12.2018

Lenders' Sacrifices under IBC, 2016:

In terms of IBC, 2016, financial creditors are entitled to CIRP against corporate debtors under section 7 which may be admitted by NCLT under section 13 which will include declaration of a moratorium under section 14 and the appointment of interim resolution professional. Unlike SICA, the moratorium period and the CIRP period is also limited in duration and cannot extend indefinitely and therefore resolution of insolvency of corporate debtors is time-bound. Under IBC, 2016, the financial creditors will constitute a Committee of Creditors which will evaluate and recommend a resolution plan submitted by the applicant for approval by NCLT. Once the resolution plan is approved by NCLT under section 31, it will be binding on the corporate debtor, its employees, members, creditors, guarantors and other stakeholders involved in the resolution plan. In case there is no approval of any resolution plan, then, the corporate debtor proceeds for liquidation in which case the right of the financial creditor to receive the distribution of the assets of the company is regulated by section 54 of IBC, which ranks secured creditors ahead of the unsecured creditors.

Although the provisions of IBC, 2016 are much more effective and time-bound than those in SICA, yet, its actual implementation remains dogged with the resolution plans approved by NCLT involving huge haircuts and sacrifices by the banks[44]. It has been held by our Supreme Court and NCLAT that initiation of CIRP is not a recovery proceeding against borrowers and is aimed at only resolving the corporate insolvency of a corporate debtor[45] and quite recently Limitation Act has also been held to be applicable to such proceedings. The Supreme Court has further ruled that if there are pre-existing disputes and if the debt is disputed then, CIRP cannot be ordered by NCLT[46] which rulings will affect the ability of banks to initiate proceedings against corporate debtors who may dispute such debt liability. Recently, the RBI had issued a circular in February 2018 disbanding all CDR schemes and urging banks to evolve a resolution plan within 180 days for those

[44] See https://www.thehindubusinessline.com/money-and-banking/bankruptcy-code-babysteps-towards-recovery-of-bad-loans/article10002680.ece visited on 16.11.2018. Also, see https://www.rediff.com/business/report/why-banks-are-uncomfortable-with-bankruptcy-code/20171004.htm as accessed on 16.11.2018

[45] *B.K. Educational Services Private Limited vs. Parag Gupta and Associates* MANU/SC/1160/2018

[46] *Transmission Corporation of Andhra Pradesh Limited vs. Equipment Conductors and Cables Limited* MANU/SC/1192/2018

borrowers who have cumulative exposure of more than Rs.2000 crores borrowings[47] and upon its failure to initiate proceedings against such borrowers under the provisions of IBC, 2016. The Bombay High Court refused to stay this direction of RBI[48], while the Allahabad High Court had stayed its operation in relation to power producing companies[49] and the Supreme Court has also refused to vacate the said stay while its application to other borrowers has been upheld by it.

Recent Practices & Conclusion:

Several laudable steps and measures have been initiated by the Government and regulators like RBI to arrest the mounting NPAs and losses accruing to the banks. Section 35 AA was inserted in the Banking Regulation Act, 1949 by way of an ordinance passed in 2017enabling the Government of India to authorize the RBI to issue directions to banks to initiate the resolution process with respect to a default under the provisions of IBC, 2016, while section 35 AB (1) was inserted to enable RBI to issue directions to banks from time to time for resolution of stressed assets, and Section 35 AB (2) enables the RBI to specify one or more authorities or committees and appoint or approve their members, to advise banks on resolution of stressed assets. The change in section 35 AB (2) is aimed at reducing the 'fear factor', particularly, of the public sector banks in taking decisions on hair-cuts for the stressed assets for disposing them off or for a OTS. At the same time, to deal with willful defaulters the provisions were made stringent by RBI through its master circular which paves way for initiation of not only recovery proceedings, but also criminal proceedings[50]. It also created a mechanism to investigate and report on frauds committed by borrowers[51]. Meanwhile, section 211 and 212 of the Companies Act, 2013 paved the way for creation of a statutory authority viz. Serious Fraud Investigation Office to effectively go into the corporate frauds by borrowers etc. Legislations like the Prevention of Money-Laundering Act, 2002, the Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act, 2015 and the Fugitive Economic Offenders

[47] RBI/2017-18/131DBR.No.BP.BC.101/21.04.048/2017-18 dated February 12, 2018
[48] *JayaswalNeco Industries Limited and Ors. vs. Reserve Bank of India and Ors.* MANU/MH/0406/
[49] *Independent Power Producers Association of India and Ors. vs. Union of India and Ors.* MANU/UP/2966/2018
[50] RBI Master Circular No. RBI/2015-16/100DBR.No.CID.BC.22/20.16.003/2015-16 dated July 1, 2015
[51] RBI Master Circular No. RBI/2015-16/75DBS.CO.CFMC.BC.No.1/23.04.001/2015-16 dated July 1, 2015

Ordinance, 2018 were some welcome legislative initiatives which, inter-alia, seek to identify, recover, tax and prosecute bank fraudsters and defaulters who flew the country without settling their bank repayments obligations or secretly hoarding them in tax heavens. Naming and shaming of the borrowers is also now well recognized by our judiciary. The Central Vigilance Commission had examined the modus operandi of top 100 banks frauds, identified the loopholes and had suggested systemic improvements in its recent report submitted in October 2018[52].

However, at the same time, both the Government and the regulators like the RBI have been fighting shy to reveal the extent of NPAs, extent of loans written-off, CDR impacts and the details of money stashed away by Indian corporates and others in tax heavens despite the receipt of and availability of such data. Information under RTI on the total extent of loans and sacrifices made by banks under the CDR schemes were refused by the Central Information Commission by holding that the CDR scheme is not a public authority[53]. The Supreme Court has reminded that RBI has a statutory duty to uphold the interest of the public at large, the depositors, the country's economy and the banking sector and thus it ought to act with transparency and not hide information that might embarrass individual banks and therefore under the provisions of the RTI Act it should disclose the information on the NPAs and loan sacrifices extended to corporate borrowers[54]. Despite the same, as neither the Government nor RBI were disclosing such details, the CIC castigated RBI and the PMO for their refusal to share the details of NPA brought about by willful defaulter and the action taken by the PMO on the letter sent to it by Raghuram Rajan, the then Governor of RBI on the subject[55]. Sadly, the RBI had filed writ petitions challenging this CIC order which forced the outgoing CIC to write to the President of India on 4th December 2018 that the Government and its regulators like RBI are intimidating the CIC against the directions issued "*to implement orders of Supreme Court confirming orders of CIC for disclosure of wilful defaulters of Banks, etc. in 11 second appeals in 2011, just to protect the names of those rich men and*

[52] Analysis of Top 100 Bank Frauds, Report dated October 15, 2018 of the Central Vigilance Commission, New Delhi
[53] *Shailesh Gandhi and Ors. vs. CDR Cell, Mumbai* (16.09.2016 - CIC) : MANU/CI/0482/2016
[54] *Reserve Bank of India and Ors. vs. Jayantilal N. Mistry and Ors.* (16.12.2015 - SC) : MANU/SC/1463/2015
[55] *Sandeep Singh Jadoun vs. CPIO, DGEAT* (16.11.2018 - CIC) : MANU/CI/0774/2018

bodies, who duped India and Indians to the tune of lakhs of crores of Rupees[56]*".* When the Apex Court was approached to regulate the matter of waivers, write-offs, rescheduling of repayments, moratoriums and one-time settlements by banks which result in loss of substantial amount of public funds, it failed to judicially legislate as it did in the *Vishaka and Ors. v. State of Rajasthan and Ors.* (MANU/SC/0786/1997), but lost the opportunity and merely proceeded to flag the issue for consideration by the Committee of Experts under the Chairmanship of Shri Vepa Kamesam, Ex-Deputy Governor of Reserve Bank of India[57]. Quite recently, the Government of India seemed to be apparently seeking to obtain from RBI a part of over Rs.3.6 lakh crores of its reserves so as to apply the same for its populist policies which was viewed as an invasion into its autonomy resulting in serious resistance from RBI[58] and also leading to recent resignation of the RBI Governor.

Although we appear to be in a tumultuous phase in relation to banking industry and there appears to be half-hearted or lackluster support from the Government and some regulators, yet the efforts under the Fugitive Economic Offenders Ordinance is paying some dividends and there is an overwhelming resolve amongst all stakeholders now to urgently arrest the continuance of NPAs, revamp the recoveries and bring to justice the fugitive economic offenders, which in the long-run will lead to improving not only the credit system but also promote honest borrowing in our country.

[56] Letter dated December 4, 2018 of Prof Dr. M Sridhar Acharayalu, who retired as Central Information Commissioner on 20 November 2018 addressed to the President of India, copy as available in https://www.moneylife.in/article/government-regulators-are-intimidating-cic-by-filing-writ-petitions-says-prof-sridhar-acharyulu/55863.html accessed on 12.12.2018.

[57] *Common Cause (A Regd. Society) vs. Union of India (UOI) and Ors.* (18.08.2010 - SC) : MANU/SC/0615/2010

[58] Speech of Dr. Viral V Acharya, Deputy Governor, Reserve Bank of India delivered in the A. D. Shroff Memorial Lecture in Mumbai on October 26, 2018

SHUT DOWNS OF ATMs- A CRITICAL ANALYSIS

KIRUTHIKA D*
&
VINESHA AM**

ABSTRACT

The banking sector is said to be the lifeblood of economic activities. This sector has changed its dimensions in various forms at lightning speed. One of the major milestones of banking sector was the introduction of Automated Teller Machine (ATM). ATM marked the first step for the digital banking in India. ATM is one of the e-banking outlets that allow customers to carry out basic transactions without the aid of any representatives. ATM is commonly called as the cash dispenser and acquired a touch point with the customers. ATMs are known to be more than machine, which would help the account holder to perform banking and withdraw money by inserting card rather than visiting the bank. The industry of ATM outsourcing has been growing exponentially in India. The ATM industry continues to move from bank's managed services to end-to-end deployment of service vendors. The services provided by the ATM industry includes ATM site sourcing, site development, electronic journal (EJ) and switch management services, managed services, maintenance services, installation services and cash management. The notification of 06.04.2018 by RBI requiring banks to put in place certain minimum standards in their arrangements with service providers by March 2019, it is feared, will result in closing down of many ATMs.

In this backdrop, the research paper examines the present status of ATMs and the reason behind the notification of RBI 06.04.2018. The authors analyze its impact on the banking industries and on the customers.

* Assistant Professor, VIT School of Law, VIT Chennai.
** 4th Year, BA LLB (Hons.), VIT School of Law, VIT Chennai.

EVOLUTION OF ATM:

The birth of ATM took place to satisfy the customer's need after the banking hours. The first ATM which resembled the modern day ATM, though did not function, was the Bankograph. This Bankograph was installed in the year 1961 in New York by the Citi Bank. It did not give out money but accepted the same without any representatives from the bank. This was not that popular but left a huge impact on the public.

The first money dispending ATM was installed on 27th June, 1967 by Barclays Bank in Enfield Town, London. It is known by the name De La Rue Automatic Cash System. Users would insert cheques into the machines and the machines would return the appropriate amount. The cheques were called tokens and they were treated with an isotope of carbon that the machine could read and interpret securely. The tokens were mailed back to users after the transactions were processed. Though not ideal by today's security standards, this system was quite popular at the time and would eventually inspire the use of plastic bank cards in ATMs[1].

The ATM that resembles the present day modern ATM was first installed on 2nd September 1969 by the Chemical Bank in New York. This ATM was the first to dispense cash using bank-issued cards that worked in combination with security keys like what we call now as PIN numbers. After the establishment of the ATMs around the world, the next concern was to go in accordance with the advancement in technology. At the advent of internet in 1990s, the next goal was to connect ATMs to the internet so that they could update automatically and quickly. ATMs have not stopped evolving since they were invented.

ATM IN INDIA:

The advent of ATMs in India took place in 1990s by the foreign banks due to the high expenses incurred for the installation of ATM and its technologies. The first Indian Bank that started introducing ATM was Indian Bank in the year 1988. The HSBC - Hongkong and

[1] Bronwyn Watt, *"How the ATM machine has evolved over the years",* available at http://paycorp.co.za/news-views/how-the-atm-machine-has-evolved-over-the-years/, accessed on 01.12.2018.

Shanghai Banking Corporation was the first foreign bank to introduce the ATM concept in India way back in 1987 at Sahar Road Branch, Andheri, Mumbai.

Originally, ATM facilities were limited to the high net worth and wealthier customers. But later when Citibank came up with the Suvidha Programme, other banks started to provide this service to all its customers without any limitation. In the first stage, banks that put up ATMs restricted their use to their own customers. A little later, some banks joined hands to run the machines and expand these services. In that phase, with its teething problems, the regulator addressed concerns relating to safety and security, especially at "offsite" ATMs, which were not attached to branches of banks.

Private Banks started to expand their networks, giving a big push to ATMs. Some of the banks started to offer free ATM cards to all customers. At that stage, banks had to still obtain approvals from the Reserve Bank of India to get around the provisions of the Banking Regulation Act that specified activities that could be carried out from the premises of a bank.

Complaints started to reach the regulator and Reserve Bank of India found that charges varied from bank to bank. RBI then set up a working group to formulate a scheme for ensuring reasonable charges, and to incorporate it in the Fair Practices Code. After completing its analysis, the RBI made all ATM transactions free, along the lines of the UK, Germany, France, among other countries.

Subsequently, however, the power to price these services returned to banks after the regulator eased its stance. But by then, the regional spread of ATMs had changed, as also the range of banking services they offered. From being just cash dispensing machines, they had started to offer payment and many other services, including for loan products, helping millions of customers reduce their visits to bank branches[2].

[2] Shaji Vikraman, "In ATM's 50th year, recalling its growth-and peak- in India", available at https://indianexpress.com/article/explained/in-bank-atm-50th-year-recalling-its-growth-and-peak-in-india-4855156/, accessed on 10.12.2018.

A Pune based technology company has developed Bio-ATM, a biometric based automated teller machine for banks and financial institutions which leverages sophisticated biometric technology to allow secure ATM transactions. This is the first time that any Indian company has developed such an ATM machine. The Bio ATM provides alternative to the regular card and pin based ATM transaction systems. In order to access accounts users need to give their biometric to the machine that will verify and authenticate it with the biometric records available in the database. The machine uses fingerprints for the verification purpose and hence customers will need to register their fingerprint with the bank[3].

The number of ATMs in the year 1999, i.e. 12 years after their birth were only around 800 ATMs in India. But the number increased from 80,117 in the year 2011 to 2,22,653 in the 2017[4]. The industry of ATM outsourcing has been growing exponentially in India, since the ATM industry continues to move from bank's managed services to end-to-end deployment of service vendors.

RBI GUIDELINES ON ATM MANAGEMENT:

The RBI's Statement on Developmental and Regulatory Policies dated 05th April, 2018 sets out various developmental and regulatory policy measures for strengthening regulation and supervision; broadening and deepening financial markets; improving currency management; promoting financial inclusion and literacy; and, facilitating data management. In para 11 of the above statement, RBI stated that in view of the increasing reliance of the banks on outsourced service providers and their sub-contractors in cash management logistics, certain minimum standards will be prescribed for the service provider/sub-contractors who are engaged by the banks for this purpose within a period of 30 days[5]. Accordingly, RBI came up with a notification on "Cash Management activities of the banks - Standards for engaging the Service Provider and its sub-contractor" dated 06th April, 2018 wherein it has been decided that the banks shall put in place certain minimum standards in their arrangements with the

[3] Refer http://shodhganga.inflibnet.ac.in/bitstream/10603/40299/5/chapter%204.pdf, accessed on 01.12.2018.
[4] Source from RBI.
[5] Refer https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=43574.

service providers for cash management related activities. Banks have been advised to review their existing outsourcing arrangements and bring them in line with these instructions within 90 days from the 06th April, 2018. The notification further stated that as the cash held with the service providers and their sub-contractors continue to remain the property of the banks and the banks are liable for all associated risks, the banks shall put in place appropriate Business Continuity Plan approved by their boards to deal with any related contingencies[6].

According to Bloomberg report, these guidelines need to be implemented by the industry and time had been given till April 2021 to transition to these rules in phases. It wants operators and banks to implement these measures by March 2019[7]. The standards prescribed by the notification are as follows[8]-

- Minimum net worth requirement of Rs.1 billion should be maintained at all times by service providers and their sub-contractors handling cash management logistics on behalf of banks.

- Minimum fleet size of 300 specifically fabricated cash vans (owned/leased).

- Cash should be transported only in the owned/leased security cash vans of the Service Provider or its first level sub-contractors. Each cash van should be a specially designed and fabricated Light Commercial Vehicle (LCV) having separate passenger and cash compartments, with a CCTV covering both compartments.

- The passenger compartment should accommodate two custodians and two armed security guards (gunmen) besides the driver.

- No cash van should move without armed guards. The gunmen must carry their weapons in a functional condition along with

[6] Refer https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11245&Mode=0

[7] Why they say half of ATMs will shut down by March next year, available at //economictimes.indiatimes.com/articleshow/66770631.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst, accessed on 11.12.2018.

[8] Supra note 6, Annex.

valid gun licenses. The Service Provider or its first level sub-contractor should also furnish the list of its employed gunmen to the police authorities concerned.

- Each cash van should be GPS enabled and monitored live with geo-fencing mapping with the additional indication of the nearest police station in the corridor for emergency.

- Each cash van should have tubeless tyres, wireless (mobile) communication and hooters. The vans should not follow the same route and timing repeatedly so as to become predictable. Predictable movement on regular routes must be discouraged. Staff should be rotated and assigned only on the day of the trip. With regard to security, additional regulations/guidelines as prescribed by Private Security Agencies (Regulation) Act, 2005, the Government of India and the State Governments from time to time must be adhered to.

- Night movement of cash vans should be discouraged. All cash movements should be carried out during daylight. There can be some relaxation in metro and urban areas though depending on the law and order situation specific to the place or the guidelines issued by the local police. If the cash van has to make a night halt, it necessarily has to be in a police station. In case of inter-state movement, changeover of security personnel at the border crossing must be pre-arranged.

- Proper documentation including a letter from the remitting bank should be carried invariably in the cash van, at all times, particularly for inter-state movement of currency.

- ATM operations should be carried out only by certified personnel who have completed minimum hours of classroom learning and training. The content of such training may be certified by a Self-Regulatory Organisation (SRO) of Cash-in-Transit (CIT) Companies/Cash Replenishment Agencies (CRAs) who may tie up

with agencies like National Skill Development Corporation for delivery of the courses.

- The staff associated with cash handling should be adequately trained and duly certified through an accreditation process. Certification could be carried out through the SRO or other designated agencies.

- Character and antecedent verification of all crew members associated with cash van movement, should be done meticulously. Strict background check of the employees should include police verification of at least the last two addresses. Such verification should be updated periodically and shared on a common database at industry level. The SRO can play a proactive role in creating a common data base for the industry. In case of dismissal of an employee, the CIT/CRA concerned should immediately inform the police with details.

- Safe and secure premises of adequate size for cash processing/handling and vaulting. The premises should be under electronic surveillance and monitoring round the clock. Technical specifications of the vault should not be inferior to the minimum standards for Chests prescribed by the Reserve Bank. The vault should be operated only in joint custody and should have colour coded bins for easier storage and retrieval of different types of contents.

- All fire safety gadgets should be available and working in the vault which should also be equipped with other standard security systems live CCTV monitoring with recording for at least 90 days, emergency alarm, burglar alarm, hotline with the nearest police station, lighting power backup and interlocking vault entry doors.

- Work area should be separate from the cash area. The premises should be under the security of armed guards whose number should have reference to the scale of operations specific to the location but not less than five in any case.

- Critical information like customer account data should be kept highly secure. Access to the switch server should be restricted to banks. Interfaces where a bank gives access to the service provider or its sub-contractor to the bank's internal server should be limited to relevant information and secured.

Adding further RBI asked banks to ensure that the computer systems in ATMs were BIOS password protected and carried supported versions of the operating system by its notification dated 21st June, 2018.

IMPACT OF ATM MANAGEMENT GUIDELINES:

The impact of the above guidelines prescribed by the Central Bank can be studied under two heads. One, their impact on the ATM industry and second, on the customers.

ATM industry:

Due to demonetization in November, 2016, the calibration of ATMs had to be changed. There were various restrictions on amount of withdrawals that can be done by account holders. This itself was a great hindrance to the ATM industry and in addition to demonetization came the above guidelines from the RBI.

The first guideline that minimum net worth requirement of Rs.1 billion should be maintained at all times by service providers and their sub-contractors handling cash management logistics on behalf of banks will create a situation where there would be very few players in the market and those would not be able to cater to the requirements of banks, even as it creates a monopoly. Of the dozens of major cash logistic companies in the county, only three namely CMS, AGS, and Checkmate, currently have net worth of Rs1 billion.

On the issue of additional armed guards, it is hard to get gun licences and increasing the number of security personnel will be difficult. Especially during elections, armed guards are in short supply. It is also impractical that loaded cash vans be parked at police stations after sundown.

As per estimates, each ATM will require three sets of five cassettes – one set in the ATM, one in transit, and another at branch/CIT company (ready for loading next day). The cost of each cassette is about Rs.20,000. So, the one-time cost of additional cassettes for over two lakh ATMs could be close to Rs.6,000 crore. Further, to comply with the minimum cash management standards, including the requirement of specially designed and fabricated Light Commercial Vehicles having separate passenger and cash compartments with CCTV covering both compartments, and two armed security guards (gunmen), prescribed by the RBI, the cost per month per ATM will increase by Rs.4,000[9]. To implement all these security, software-hardware directive would entail an additional cost of minimum Rs.150,000 per ATM per month[10].

These requirements were never anticipated by the industry participants at the time of signing contracts with the banks. Many of these agreements were inked four to five years ago[11].

Almost 50 per cent of the 2.22 lakh ATMs may have to be closed by March 2019 on account of non-viability of operations brought about by recent regulatory guidelines for ATM hardware and software upgrades, recent mandates on cash management standards, and the cassette swap method of loading cash.

Customers:

It is obvious that such move of the Central Bank is for protecting the interest of the general public and the customers in particular. But, if the guideline lead to the closure of ATMs then that would have a negative impact on the customers for whom the banking industry is existing.

Consumers would first face the difficulties of using the normal banking system again by going back to banks and to wait in long queue to get their banking works to be done. As not everyone would adopt

[9] See https://www.thehindubusinessline.com/money-and-banking/catmi-tells-rbi-to-constitute-task-force-on- pricing-to-prevent-closure-of-atms/article25579967.ece, accessed on 05.12.2018.

[10] See https://www.ndtv.com/india-news/atm-shutdown-50-atms-in-india-may-shut-down-by-march-next-year-says-report-1951093, accessed on 09.12.2018.

[11] See https://www.livemint.com/Politics/pc0J8nfD5m9Ze1mnHWYLaL/50-of-existing-ATMs-across-India-to-shut-down-by-March-2019.html, accessed on 02.12.2018.

themselves to the concept of internet banking for various reasons like, few may not know how to use such technology; some may not utilize such facilities. It may also happen that individuals, who are able to utilize them, step back because of the high number of online fraud and wrong transactions that might happen.

The enhanced charges will increase by 30-40 per cent for security alone. The per-transaction charge might increase by Rs.6 to Rs.10. This might increase interchange fee, currently capped at Rs.15 per transaction[12]. Services such as the doorstep cash-delivery and pick-up, offered to senior citizens and small businesses, would also be affected. Cash loading will be affected.

Closure of ATM would impact on jobs of many individuals and also the financial inclusion efforts of the government. There would be a negative impact on the financial inclusion programme where the beneficiaries under the scheme withdraw their cash subsidies from ATMs. Thousands of families many lose their jobs and this will result in huge unemployment, from the security guards to many officials authorities. It would be like hitting hard both urban and rural population, and dealing a blow to the digitization policy.

Using internet banking as a result of shut downs of ATM's would pave way for crime crimes. Fraudulent money transfer would begin and many new regulations and new method of transaction may have to be passed on it to reduce and govern on the transaction online.

CONCLUSION:

Closing half the ATMs in the country would mean another demonetisation-like situation where people struggle to get hold of cash. Shutting down of ATM's would be detrimental to financial services in the economy as a whole. 30% of the account holders in bank are regular users of ATM's, now this would also disturb the customers of those banks. ATM's are known to be the financial connectivity among people, only after the setting ups of ATM's financial transactions,

[12] Raghu Mohan, RBI's new cash logistics norms might disrupt functioning of ATMs: IBA, available at https://smartinvestor.business-standard.com/market/story-542593-storydet-RBIs_new_cash_logistics_norms_might_disrupt_functioning_of_ATMs_IBA.htm#.XBktuzAzbIU, accessed on 12.12.2018.

withdrawals and deposits of cash was made easier and simple for the customers.

Despite the growth of cards and other payment systems, the market for cash, and ATMs to dispense it, does seem likely to remain strong in India. As a business historian and expert on cash economies, Batiz-Lazo pointed out the ratio of ATMs to population in India is still way below global norms, leaving plenty of scope to expand. Once you leave the metros, ATMs still seem far too few and remote[13]. A report by Hexa research suggests that the worldwide ATM market is projected to garner more than 26 billion US$ by 2024, growing at around 9.8% CAGR in the forecast period (2016-2024). It had a value of 12.5 billion US$ in 2015. Technological breakthroughs and innovative security standards amid growing wireless devices should propel the market in the near future. This can reduce fraud and lead to safe financial transactions[14].

The Confederation of ATM Industry has called upon the Reserve Bank of India (RBI) to constitute a task force to transparently discover pricing related to implementing cassette swap for replenishing cash and adhering to minimum standards for cash-management activities. The only way to salvage the situation for the industry is if banks step in to bear the load of the additional cost of compliance. Also the RBI should relax net worth and security rules to prevent interchange costs from shooting up.

[13] "Here's the story of ATMs over the years", available at https://economictimes.indiatimes.com/slideshows/nation-world/heres-the-story-of-atms-over-the-years/miles-to-go/slideshow/55511202.cms, accessed on 03.12.2018.

[14] See https://www.hexaresearch.com/research-report/atm-market.

ANALYSIS OF NEW TRENDS IN BANK: CUSTOMER RELATIONSHIP

VIGNESHWARAN.R*
&
RAJPRIYA.R

ABSTRACT

Indian economic environment is witnessing path breaking reform measures. Today the banking industry is stronger and capable of withstanding the pressures of competition. We are having a fairly well developed banking system with different classes of banks, both old and new generation, with the Reserve Bank of India as the fountain Head of the system. In the banking field, there has been an unprecedented growth and diversification of banking industry has been so stupendous that it has no parallel in the annals of banking anywhere in the world. In general, banks have had a track record of innovation, growth and value creation. However this process of banking development needs to be taken forward to serve the larger need of financial inclusion through expansion of banking services, given their low penetration as compared to other markets. Now-a-days we are hearing about e-governance, e-mail, e-commerce, e-tail etc. In the same manner, a new technology is being developed in US for introduction of e-cheque, which will eventually replace the conventional paper cheque. Our Indian banks have developed new trends for the growth of their banks, as to attract the customers. This paper deals with the new trends of banks and relation between the bank and customers and its backdrops.

INTRODUCTION

During the last 41 years since 1969, tremendous changes have taken place in the banking industry. The banks have shed their traditional methods, improving and coming out with new types of services to cater to the emerging needs of their customers. Today, we are having a fairly well developed banking system with different classes of banks – public sector banks, foreign banks, private sector banks – both old and new generation, regional rural banks and co-operative banks with the Reserve Bank of India as the fountain Head of the system. Some of them have engaged in the areas of consumer

* DR. Ambedkar Global Law Institute, Tirupathi – AP.

credit, credit cards, merchant banking, leasing, mutual funds etc. A few banks have already set up subsidiaries for merchant banking, leasing and mutual funds and many more are in the process of doing so. The banking system in India is significantly different from other Asian nations because of the country's unique geographic, social, and economic characteristics. Today, Indian banking industry is one of the largest in the world. Customer Relationship Management (CRM) in the banking sector is of strategic importance. CRM is a holistic process of acquiring, retaining, and growing customers. CRM is used to define the process of creating and maintaining relationships with business or customers.

1. TO UNDERSTAND THE RECENT TRENDS IN "CRM"

- CRM IN BANKING SECTOR

Good customer service is brand investor of any bank. The idea of CRM is that it helps banks use technology and human resources to evaluate the perception of customers and the value of those customers. Customer Relationship Management is very important for the growth and profitability of banks in the present technological age. The definition of CRM given as "the market place of the future" is undergoing a "technology-driven metamorphosis". It is emphasized that customer relationship management based on social exchange and equity significantly assists the firm in developing collaborative, cooperative and profitable long-term relationships. CRM is instrumental in identifying and capturing the most customers of the bank. It combines technology with human resources in order to create new strategies to acquire new customers and retain the existing ones. The long-term business relationships provide many potential benefits for banks and clients.

GLOBAL BANKING DEVELOPMENTS

The year 2010-11 was a difficult period for the global banking system, with challenges arising from the global financial system as well as the emerging fiscal and economic growth scenarios across countries. Global banks exhibited some improvements in capital adequacy but were beleaguered by weak credit growth, high leverage and poor asset quality. In contrast, in major emerging economies, credit growth remained at relatively high levels, which was regarded as a cause of concern given the increasing inflationary pressures and

capital inflows in these economies. In the advanced economies, credit availability remained particularly constrained for small and medium enterprises and the usage of banking services also stood at a low, signalling financial exclusion of the population in the post-crisis period. On the positive side, both advanced and emerging economies, individually, and multi-laterally, moved forward towards effective systemic risk management involving initiatives for improving the macro-prudential regulatory framework and reforms related to systemically important financial institutions.

RECENT TRENDS IN BANKING

Through the years, the CRM industry relied heavily on technology and software developments. CRM has evolved over the decades. The term became popular in the early '90s, when it began to be used to refer to front-office applications. Banks can develop innovative and creative customer solutions to attain growth and profitability along with sound risk-management practices. The CRM industry relied heavily on technology and software developments. CRM trends in the coming months - and years - are bound to change how businesses deal with customers. Cloud CRM and social CRM are used recently to deal with customers. CRM products such as Sales force, Microsoft Dynamics CRM, Exact Target, Markets, Silver Pop, Oracle and SAP are available in the market. Public sector banks must use these CRM techniques to remain in competition. The following are some of the latest e-CRM techniques used by banks in offering new products and services to its customers.

1) Electronic Payment Services (E Cheques)
2) Real Time Gross Settlement (RTGS)
3) Electronic Funds Transfer (EFT)
4) Electronic clearing services (ECS)
5) Automatic Teller Machine (ATM)
6) Point of Sale Terminal
7) Tele Banking
8) Electronic Data Interchange (EDI)
9) Mobile banking
10) Chip card

1) Electronic Payment Services – e- Cheques

A new technology is being developed in US for introduction of e-cheque, which will eventually replace the conventional paper cheque. India, as harbinger to the introduction of e-cheque, the Negotiable Instruments Act has already been amended to include; truncated cheque and e-cheque instruments.

2) Real Time Gross Settlement (RTGS)

Real Time Gross Settlement system, introduced in India since March 2004, is a system through which electronic instructions can be given by banks to transfer funds from their account to the account of another bank. The RTGS system is maintained and operated by the RBI and provides a means of efficient and faster funds transfer among banks facilitating their financial operations. As the name suggests, funds transfer between banks takes place on a 'Real Time' basis. Therefore, money can reach the beneficiary instantaneously and the beneficiary's bank has the responsibility to credit the beneficiary's account within two hours.

3) Electronic Funds Transfer (EFT)

Electronic Funds Transfer (EFT) is a system whereby anyone who wants to make payment to another person/company etc. can do so by giving complete details such as the receiver's name, bank account number, account type (savings or current account), bank name, city, branch name etc.

4) Electronic Clearing Service (ECS)

Electronic Clearing Service is a retail payment system that can be used to make bulk payments/receipts of a similar nature especially where each individual payment is of a repetitive nature and of relatively smaller amount. This facility is meant for companies and government departments to make/receive large volumes of payments rather than for funds transfers by individuals.

5) Automatic Teller Machine (ATM)

1. ATM is a step in improvement in customer service.
2. ATM facility is available to the customer 24 hours a day. The customer is issued an ATM card.
3. This is a plastic card, which bears the customer's name. This card is magnetically coded and can be read by this machine.

4. After the card is a recognized by the machine, the customer enters his personal identification number.
5. When the transaction is completed, the ATM ejects the customer's card.

6) Point of Sale Terminal

During a transaction, the customer's account is debited and the retailer's account is credited by the computer for the amount of purchase.

7) Tele Banking

Tele Banking facilitates the customer to do entire non-cash related banking on telephone. Under this devise Automatic Voice Recorder is used for simpler queries and transactions. For complicated queries and transactions, manned phone terminals are used.

8) Electronic Data Interchange (EDI)

Electronic Data Interchange is the electronic exchange of business documents like purchase order, invoices, shipping notices, receiving advices etc. in a standard, computer processed, universally accepted format between trading partners.

9) Mobile banking

Mobile banking facility is an extension of internet banking. The bank is in association with the cellular service providers who offer this service. For this service, mobile phone should either be SMS or WAP enabled.

10) Chip Card

The customer of the bank is provided with a special type of credit card which bears customer's name, code etc. The credit amount of the customer account is written on the card with magnetic chips. The computer can read these magnetic spots.

INNOVATIONS

Advances have been made in automated decision-making methodologies, and there are some projections that many manual tasks will be machine-controlled after about five years from now.

Innovations concentrate on 'customer experience', impacting in the following areas**.**

- Assessment of special services: approval of new accounts, loans and mortgages. The purely deterministic processes that result in "Computer says NO!" are not acceptable.
- Advancement in the sophistication of so-called 'robo-advisors' for investment advice, mainly using pattern-matching techniques, and superseding the analyst's ability to define use-cases.
- Adaptive systems that can "learn" from new data.
- Fraud detection by identifying unusual transactions, patterns and styles.

CRM IMPLEMENTATION

For CRM to be truly effective a bank must first decide what kind of customer information it is looking for and it must decide what it intends to do with that information. It doesn't happen by simply buying software and installing it. To ensure the proper functioning customer relationship management concept and for successfully implementation in banking sector, following requirements should be complied:

- There should be customer-focused organisation and infrastructure.
- Banks have to assess accurate picture of customer categories.
- Banks have to evaluate the lifetime value of customers.
- Banks should maximize the profitability of each customer relationship.
- Understand how to attract and keep the best customers.
- Maximise ROI on marketing campaigns.

Social networking sites are always changing user and customer experience, and innovating to meet customers' changing demands. Customers now have the tools to express their opinions on anything, at anytime and anywhere in the world. This has changed the role of customer feedback, and made it much more important;

after all, customer feedback over social media has been known to make or break businesses. As a result, business entities are increasingly growing aware of the power of social media as a method for engaging customers and potential customers. Mobility is also creating technology and marketing trends thanks to the emergence of smart phones and tablets.

CRM in the Future

The marketing and technology aspects of CRM will potentially grow in coming years. Companies looking to harness the power of customer relationships should pursue strategies that are most in line with the type of customers they have and the type they want to gain. Thanks to social media and increasing interaction between people and products online, customers' opinions about the products or services they use have become a business driver. As a result, companies must listen and respond to what people are saying and harness the power of current technology to continue to anticipate and deliver what their customers want.

BACKDROPS OF NEW TRENDS IN BANKING SYSTEM

The customer service arena is undergoing an enormous shift. Digital transformation, and the widespread availability of new technologies, is rapidly changing the way customers and banks interact. Indeed, for many successful banks, customer service has gone from being an afterthought or IT issue to a central part of the bank's strategy and offering.

There must be *multiple channels to contact the banks* "Customers must choose the ways in which they interact and have become less tolerant of organizations that fail to integrate their operational channels into a faultless, coherent set of experiences," As the time has changed customer priorities and expectation have also changed though technology has developed and we reach everything within our finger tips but there are many rural people who aren't aware. It might be easy to think that customer service through social media is something for younger generations, while older generations prefer written communications. While *customer service through social media* is indeed more prevalent among younger demographics, it's not solely limited to this age group. Conversely, customer service by phone is still an important tool and point of contact among younger

generations, who still want personal contact and service. There must be a greater importance placed on customer service. Banks themselves must react and place greater importance on the role and function of customer service within their organization. It's shifting from being a sideline topic to the heart of many successful banks, who know that it's important to put the customer at the heart of customer service.

Drawbacks of Internet Banking

The current trend of exclusively using the online mode to make all kinds of transactions has a few pitfalls which may prove costly in the long run unless guarded against from the beginning.

Online transactions take a toll on the relationship with the banker which the traditional visit to the branch office used to foster. Personal relationship with the staff at the banks comes handy when requesting for faster loan approval or a special service which may not be available to the public. The manager has many discretionary powers such as waiving of penal interest or service fees which were often taken advantage of by better acquaintance with the staff. Additionally personal contact also meant that the banker would provide essential financial advice and insights which are beneficial to the customer.

Complex Transactions: There are many complex transactions which cannot be sorted out unless there is a face to face discussion with the manager that is not possible through internet banking. Solving specific issues and complaints requires physical visit to the bank and cannot be achieved through the internet. Online communication is neither clear nor pin pointed to help resolve many complex service issues. Certain services such as the notarization and bank signature guarantee cannot be accomplished online. On the other hand, the evolution of modern technology has disadvantages, for example, dependence on new technology. Man no longer needs to think. Even if the calculator is a good invention, man no longer makes mental calculation and no longer works his memory. The decline of human capital implies an increase in unemployment. In some areas, devices can replace the human mind.

The use of technology certainly needs rule and new laws. For example internet use is an individual freedom. However, the invention

of the atomic bomb cannot be an individual freedom. In fact, regulations are difficult to implement when these technologies are introduced – such as regulation surrounding the impending arrival of autonomous vehicles.

Finally, as most technological discoveries aim to reduce human effort, it would imply that more work is done by machines. This equates to less work for people: the human is becoming ever so obsolete by the day, as processes become automated and jobs are made redundant.

The negative impact of the influence of technology on children should not be underestimated as well.

SAFEGUARDING CUSTOMER INFORMATION

Adding to this complexity, customer privacy and information security are under attack as never before. The threats come from many quarters: thieves, constant phishing expeditions by criminals seeking to trap unwary customers, and even "inside jobs" where staff sells customer data to criminals. Expanding legislative and industry requirements for customer security are also increasing costs for financial services companies. Compliance with customer information regulations is becoming increasingly complex as regulations are growing at all operating levels. In this context it is vital that banks ensure their customer data is secure from both internal and external threats. By preventing security breaches and avoiding losses, banks can actually realize a ROI from investing in security. This makes protecting customer data a prerequisite for competing effectively in the retail financial services market. Banks must balance the cost of security against the need to share information and service the customer, while at the same time finding ways to secure vital customer and financial data for the purpose of risk management.

CONCLUSION

Retail Banking deals with lending money to consumers which include a wide variety of loans, including credit cards, mortgage loans and auto loans. Retail Banking refers to banking in which banking institutions execute transactions directly with consumers,

rather than corporations or other entities. It is generally conceived to be the provision of mass market banking services to private individuals. It has expanded over the years to include in many cases services provided to small and medium sized business. Retail banking is the fastest growing sector of the banking industry with the key success by attending directly the needs of the end customers. It holds a glorious future in coming years. Retail banking sector as a whole is facing a lot of competition ever since financial sector reforms were started in the country. Walk-in-business is a thing of past and banks are now on their toes to capture business. Banks therefore, are now competing for increasing their retail business. There is a need for constant innovation in retail banking. This requires product development and differentiation, micro planning, marketing, product pricing, customization, technological upgradation, home/electronic/mobile banking, effective risk management and asset liability management techniques. While retail banking offers phenomenal opportunities for growth, the challenges are equally discouraging. How far the retail banking is able to lead growth of banking industry in future would depend upon the capacity building of banks to meet the challenges and make use of opportunities profitably.

SUGGESTIONS

1. The need for retail banking services provided by public sector banks is to improve their speed and efficiency of service delivery in a secure environment.

2. There is need to improve the quality of service delivery in such areas as accuracy in customer accounts management and, excellent and cordial banker-customer relationships by public sector banks.

3. In order to have confidence of customer, the public sector banks have to consciously cultivate the habit of treating their customer as king. This would include provision of more and more customized services that are tailor-made to suit their individual needs.

4. The service quality dimension “Reliability” is defined by the promise to do, problem solving techniques, performed service right to the first time, and error free records. The dimension

"reliability" is associated with the bank's ability to perform the promised service accurately and dependably. Performing the services dependably and accurately is the heart of service marketing excellence. Although there is no doubt that the public sector banks have been acquiring the large number of customers as compared to private sector banks, the customers of private sector banks feel more satisfaction regarding the Reliability dimension.

5. Banks should observe the RBI norms and provide facilities as per the norms which are not being followed by the banks. While the customer must be given prompt services and the bank officer should not have any fear on mind to provide the facilities as per RBI norms to the units going sick.

6. Banks should provide loans at lower interest rates and education loans should be given with ease without much documentation. All the banks must provide loans against shares. For fair dealing with the customers, the staff should be cooperative, friendly and must be capable of understanding the problems of customers.

7. Internet banking facility must be made available in all the banks. Prompt dealing with permanent customers and speedy transaction without harassing the customers would enhance the image of the banks.

8. Each section of every bank should be computerized even in rural areas also. Real Time Gross Settlement can play a very important role to enhance the retail services by public sector banks.

9. More ATM coverage should be provided for the convenience of the customers. No limit should be placed on cash withdrawals on ATM cards.

10. 24 hours banking should be introduced so as to facilitate the customers who may not have a free time in the day. It will help in facing the competition more effectively.

11. The charges for saving account opening are high, so they should also be reduced. Banks should increase the rate of saving account.

12. Customers generally complain that full knowledge is not provided to them. Thus the bank should properly disclose the

features of the product and services to the customers. Moreover door to door services can also be introduced by bank.

13. The need of the customer should properly be understood so that customer feels satisfied. The relationship value should be maintained. Branch should promote cooperation and coordination among employees which help them in efficient working.

The paper had incorporated time factor, human relation approach of bank employees, the enquiries and the employee response, knowledge and skill of the employees as indicators of good customer satisfaction. These variables were systematically weighed in determining the customer satisfaction. This study would definitely enable the bank authorities to bring this to the notice of bank employees who must shoulder the moral responsibilities for the growth and development of the country, in retail banking industry in particular.

REFERENCE:

1. Dr. S.R. Myneni –law of banking
2. file:///C:/Users/aswathishaju/Desktop/penzugy_Biro_Balazs.pdf
3. https://www.cbronline.com/opinion/crm-trends-2018
4. https://www.marketingtechnews.net/news/2016/dec/06/five-emerging-customer-service-trends-and-what-do-about-them/
5. file:///C:/Users/aswathishaju/Desktop/98.pdf
6. file:///C:/Users/aswathishaju/Desktop/82bfce4c46ce89d241be767ab7f4022b9fc2.pdf
7. https://www.sapling.com
8. file:///C:/Users/aswathishaju/Desktop/1705.10974.pdf
9. file:///C:/Users/aswathishaju/Desktop/98.pdfv
10. https://www.google.com/search?

11. file:///C:/Users/aswathishaju/Desktop/82bfce4c46ce89d241be767ab7f4022b9fc2.pdf
12. file:///C:/Users/aswathishaju/Desktop/82bfce4c46ce89d241be767ab7f4022b9fc2.pdfv
13. Dr. Anjani Kant - Lectures on Banking Law for law students
14. R.N. Chanudhary - Banking law
15. Seth`s - commentaries on banking act along with allied banking laws
16. Ravi Shined - lectures on law of banking
17. Dr.A. Subranhmanyam - law of banking
18. P.N. Varshney - banking law and practice
19. S.N. Maheawari, R.R. Paul-banking theory and law and practice
20. Dr.K. Nirmala Prasad, J. Chandradass - banking and financial system
21. Anoopam modak - Supreme court on banking and finance laws
22. M.L.Tannan-banking law practice in India

CYBER ATTACKS ON INTERNET BANKING AND COUNTERMEASURES

R.S. SURIYA*

INTRODUCTION:

As the new millennium and information age progress, organizations around the world are going through massive transformation efforts to cope with the constantly changing business market trends .Volatile financial markets have all added to the pressure on organizations to come up with effective responses to survive and succeed. Technology trends and a shift to digital business, accompanied with the revolution in the smart systems, have caused a massive re-positioning of the financial services market from a fundamentally labour-based model to an automated process-driven business model. Information technology has played very important role in the field of banking. Online banking or e-banking is an electronic payment system that enables customers of a financial institution to conduct financial transactions on a website operated by the institution, such as a retail bank, virtual bank, credit union or building society. Banking in India in the modern sense originated in the last decade of the 18th Century[1]. Since that time the banking sector had been applying different ways to provide facilities to a common man regarding money. The banking sector is totally changed after the arrival of Internet. Convergence of technologies has made the distribution of services more convenient than ever before. Automatic Teller Machines, bill payment kiosks, internet based services and phone based services (both voice and text), automated hotel check out, automated check-in for flights, automated food ordering system in restaurants, vending machines, Interactive voice response systems are examples of technology based service delivery channels[2]. Amongst various service industries, banks sector has been mostly influenced by the information technology.

* V-C, B.A. B.L (Hons), School of Excellence in Law.

1 Manisha M. More and Dr.K M. Nalawade (2014): Cyber Crimes and Attacks: The Current Scenario, 1st National Conference organized by NESGOI, Pune.

2 History of Banking: http://en.wikipedia.org.wiki/Banking_in_India.

INFORMATION TECHNOLOGY AND INDIAN BANKING SECTOR

The Indian banking system has come a long way since independence from nationalization to liberalization. It has witnessed transition from a slow business institution to a highly proactive and dynamic entity. This transformation has been largely brought about by liberalization and economic reforms that allowed banks to explore new business opportunities rather than generating revenues from conventional streams of borrowing and lending. A high-level committee was formed under the chairmanship of Dr.C. Rangarajan, to draw up a phased plan for computerization and mechanization in the banking industry. The focus was on customer service. For this purpose, two models of branch automation were developed and implemented. The second Rangarajan committee constituted in 1988 drew up a plan for computerization and automation to other areas such as funds transfer, e-mail, BANKNET, SWIFT, ATMs, i-banking etc. In the last decade, information technology has brought significant changes in the banking sector.[3] It has provided an opportunity to banks for offering differentiated products and services to their customers using technology platforms. Apart from operations, advancement in technology has played an important role in the distribution strategy of commercial banks.

INTERNET BANKING IN INDIA:

The role of Internet is becoming inevitable in a society. The Internet banking is changing the environment of banking industry and is having the major effect on banking relationships. Initially, banks promoted their core capabilities, being products, channels and advice, through the Internet. Then, they entered internet commerce market as providers/distributors of their own products and services. The trend toward electronic delivery of products and services is occurring dramatically in the financial service industry where the shift is partly a result of consumer demand, but also of a ruthlessly competitive environment. More recently, due to advances in Internet security and the advent of relevant protocols[4] (e.g. Integrion, OFX, SET etc.), banks

[3] Cyber crime News:http://www.computerweekly.com/news/2240215532.Financial-services-sector-attract-most-cyber-crime.

[4] Markson, T. & Hokenson, M. University of Michigan Business Case Study, December 2003.

discovered that they can play again their primary role as financial intermediates and facilitators of complete commercial transactions via electronic networks and especially via the Internet. Currently, there are three basic kinds of Internet banking technologies that are being employed in the marketplace:[5]

- Information,
- Communication, and
- Transaction.

In general, these Internet sites offer only the most basic services. 55% are so called 'entry level' sites, offering a little more than company information and basic marketing materials. Only 8% offer 'advanced transactions' such as online funds transfer, transactions & cash management services. Foreign & Private Banks are much advanced in terms of the number of sites & their level of development. Internet Banking is the new generation of banking in India. Most private and MNC banks have already setup an elaborate Internet banking infrastructure.

THE EVOLVING CYBER THREAT LANDSCAPE:

E-banking implies provision of banking products and services through electronic delivery channels. It is a method of banking in which the customer conducts transactions electronically via the Internet. It is also known as electronic funds transfer (EFT), is simply the use of electronic means to transfer funds directly from one account to another, rather than by check or cash.

The high connectivity to the world from any place has developed many crimes and these increased offences. Cyber Crimes Attack, also called Computer Network Attack, is an attack from one computer to another computer using a network deliberately to alter, disrupt, deny, degrade or destroy or damage the data hosted in the attacked system or network. The interrupter interrupts by producing a malicious code which is directed against a computer processing code or logic. These attacks are made in a way to steal the relevant information without leaving back any traces of intrusion. Financial crime, also referred as

[5] www.banknetindia.com.

white-collar crime, covers a wide range of criminal offences which are generally international in nature.[6] Cyber attacks generally refer to criminal activity conducted via the Internet. These crimes affect private individuals, companies, organizations and even nations, and have a negative impact on the entire economic and social system through the considerable loss of money incurred. These attacks can include stealing an organization's intellectual property, confiscating online bank accounts, creating and distributing viruses on other computers, posting confidential business information on the Internet and disrupting a country's critical national infrastructure. The loss or misuse of information assets is the most significant consequence of a cyber attack.

RISKS INVOLVED IN INTERNET BANKING:

Internet banking risks consist of risks associated with credit, interest rate, transaction, liquidity risk, price risk, transaction risk, etc. Some of the important risks involved in the Internet banking are:[7]

1. Credit Risk

Customers can reach from anywhere, challenging for institutions to verify the bona fides of their customers, which is an important element in making sound credit decisions.

2. Liquidity Risk

Increase deposit volatility from customers who maintain accounts solely on the basis of rate or terms.

3. Interest Rate Risk

Interest rate risk arises from differences between the timing of rate changes and the timing of cash flows reprising risk.

4. Foreign Exchange Risk

[6] Rajkumar, Manisha Jitendra Nene, ―A Survey on Latest DoS Attacks: Classification and Defence Mechanisms‖, International Journal of Innovative Research in Computer and Communication Engineering,vol. 1,no. 8, pp. 1847-1860,2013.

[7] Supranamaya Ranjan, Ram Swaminathan, Mustafa Uysal and Edward Knightly, ―DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection‖, In Proc. Of IEEE Infocom, 2006, pp.23-29.

Foreign exchange risk is present when a loan or portfolio of loans is denominated in a foreign currency or is funded by borrowings in another currency.

5. Compliance Risk

Compliance risk is the risk to earnings or capital arising from violations of, or non-conformity with laws, rules, regulations, prescribed practices, or ethical standards.

6. Strategic Risk

Strategic risk is the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes.

7. Reputation Risk

Reputation risk is the current and prospective impact on earnings and capital arising from negative public opinion.

SECURITY AND PRIVACY THREATS IN INTERNET BANKING[8]:

When the internet was developed, the founding fathers of internet hardly had any inclination that internet could also be misused for criminal activities. Since the beginning of the year 2004, reports of fraud cases have nearly exploded especially in internet banking.[9] Major internet banking threats are discussed as under:

- **Phishing Attacks**

Phishing is an attempt by fraudsters to 'fish' for banking details of customers. A phishing attempt usually is in the form of an e-mail that appears to be from customer‘s bank. The e-mail usually encourages customer to click a link in it that takes him to a fraudulent log-in page designed to capture authentication details such as password and Login ID. E-mail addresses can be obtained from publicly available sources or through randomly generated lists.

---

[8] Huey-Ing Liu and Kuo-Chao Chang, ―Defending Systems Against Tilt DDoS Attacks‖, The 6th International Conference on Telecommunication Systems, Services, and Applications, Bali, 2011, pp.22-27.

[9] Online Banking: Threats and Countermeasures‖, Ahnlab Online Security Available: https://sqnetworks.com/.

- **Spoofing**

Website spoofing is the act of creating a website, as a hoax, with the intention of performing fraud. To make spoof sites seem legitimate, phishers use the names, logos, graphics and even code of the actual website. They can even fake the URL that appears in the address field at the top of your browser window and the Padlock icon that appears at the bottom right corner.

- **Vishing**

Vishing is a combination of Voice and Phishing that uses Voice over Internet Protocol (VoIP) technology wherein fraudsters feigning to represent real companies such as banks attempt to trick unsuspecting customers into providing their personal and financial details over the phone.

- **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.

- ***Spam e-mails***

Spam emails are unsolicited emails or junk newsgroup postings. Spam emails are sent without the consent of the receiver— potentially creating a wide range of problems if they are not filtered appropriately.

- **Trojan**

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.

- ***Denial-of service***

DoS occurs when criminals attempt to bring down or cripple individual websites, computers or networks, often by flooding them with messages.

- **Malware**

Malware is software that takes control of any individual's computer to spread a bug to other people's devices or social networking profiles. Such software can also be used to create a botnet a network of computers controlled remotely by hackers, known as herders to spread spam or viruses.

Scare war

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.

- **Fiscal Fraud**

By targeting official online payment channels, cyber attackers can hamper processes such as tax collection or make fraudulent claims for benefits.

- ***State cyber attacks***

Experts believe that some government agencies may also be using cyber attacks as a new means of warfare. One such attack occurred in 2010, when a computer virus called Stuxnet was used to carry out an invisible attack on Iran's secret nuclear program. The virus was aimed at disabling Iran's uranium enrichment centrifuges.

- **Carders**

Stealing bank or credit card details is another major cyber crime. Duplicate cards are then used to withdraw cash at ATMs or in shops.

- ***Cross site scripting***

Cross-site scripting (XSS) is a kind of cyber security vulnerability usually found in web applications and they allow code injections by malicious web users into the web pages that are viewed by other users. Examples of such code include client-side scripts, HTML code, etc. A cross-site scripting vulnerability can be exploited by attackers to bypass access controls. Their impact ranges from a petty nuisance to a significant security risk, depending on the sensitivity of the data that is handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner.

- ***Cyber Squatting***

Cyber-squatting is a process in which a famous domain name is registered and then it is sold for a fortune. Cyber Squatters register domain names which are similar to popular service providers' domains so as to attract their users and benefit from it. Some countries have specific laws against cyber-squatting that are beyond the normal rules of trademark law.

- ***SMS Spoofing***

It is a relatively new technology in which a user receives a SMS message on phone which appears to be coming from a legitimate bank. In this SMS the originating mobile number (Sender ID) is replaced by alphanumeric text. Here a user may be fooled to give his/her online credentials and his/her money may be at risk of theft.

CYBER-CRIME SAFETY MECHANISMS USED BY BANKS

The models currently adopted in online banking systems are based on several security layers, consisting of diverse parallel solutions and mechanisms which aim at protecting the banking application and the user's data, providing identification, authentication and authorization.[10] These are:

1. Digital Certificates

[10] Catherine weir, Irain Mc Kay, Mervyn Jack, "Functionality and usability in design for e- Statements in e-Banking services", Volume 19, Issue 2, March, 2007.

Digital certificates are used to authenticate both the users and the banking system itself. This kind of authentication depends on the existence of a Public Key Infrastructure (PKI) and a Certificate Authority (CA), which represents a trusted third-party who signs the certificates attesting their validity.

2. One-Time Password Tokens

One-Time Password devices are commonly used as a second authentication factor, which may be requested in specific or random situations. This kind of devices render captured authentication data useless for future attacks through the use of dynamically changing passwords which can be used only once.

3. One-Time Password Cards

This constitutes a less expensive method for generating dynamic passwords, also providing a second authentication factor. However, in some banking systems, passwords generated by OTP cards are reused a number of times before being discarded, rendering this system vulnerable to short term replay attacks[11].

4. Browser Protection

In this model, the system is secured at the Internet browser level, which is used to access the banking system. The user and his browser are protected against known malware by monitoring the memory area allocated by the browser in order to detect such malware and hinder credential theft and capturing of sensitive information.

5. Virtual Keyboards

Virtual keyboards were developed for the efficient use of key loggers (which capture information typed into the device). These devices are usually based on Java and software based cryptography, allowing portability between different devices. Currently they are being replaced by other more efficient methods which require less processing power and slower transmission rates.

[11] Navjeet Kaur, ―A Survey on Online Banking System Attacks and its Countermeasures‖, International Journal of Computer Science and Network Security, vol.15, no.3, pp. 57-61, 2015.

6. Device Registering

This method restricts access to the banking system to previously known and registered devices. Hardware fingerprinting techniques are used in conjunction with user identification through secret credentials.

7. Captcha

Completely Automated Public Turing test to tell Computers and Humans Apart, is a method recently adopted in some banking systems whose objective is to render automated attacks against authenticated sessions ineffective. This method requires the legitimate user to input information conveyed as scrambled images which are difficult for automated robots to process and recognize.12[12]

8. Short Message Service (SMS)

This method has been applied in some banking systems to notify users about transactions requiring their authorization. It provides a second authentication channel for transactions that fit certain characteristics by sending to the user a set of characters which have to inform in order to authorize and process the transaction through the online banking system.

9. Device Identification

Device identification is usually applied together with device registering but it is also used as a stand-alone solution in online banking systems that aim at facilitating user access. This identification model is based on physical characteristics of the user's device through which it is possible to identify its origin and history information.

10. Positive Identification

Positive identification is a model where the user is required to input some secret information only known to him in order to identify itself. It is applied as a second authentication method.

[12] Liao, Z., & Cheung M., "Challenges to Internet E- Banking", Communications of the ACM, 46(12), 248-250, 2003.

11. Pass-Phrase

It is a security model based on information held by the user. It is usually used as a second authentication method in transaction that involves money movement.

12. Transaction Monitoring

Even though this method is not thoroughly analyzed in the present work, it is currently applied in all online banking systems, each of them using different techniques. Artificial intelligence, transaction history analysis and other methods that identify fraud patterns in previously processed transactions are among the various approaches to transaction monitoring.

CHALLENGES IN THE CURRENT SYSTEM OF PROTECTION:

The following are some challenges of cyber crimes related to mobile and online banking:

1. Tracking the origin of crime- Tracing cyber criminals is very difficult because criminal investigations and criminal activity itself is borderless by nature.

2. Growth of the underground cyber crime economy - The fight against cyber crime has revealed the growth of an underground cyber crime economy. The underground economy attracts many digital experts and talented individuals with a specialty around cyber initiatives.

3. Shortage of skilled cyber crime fighters - Skilled manpower is required for implementing cyber security measures and encountering cyber attacks.

4. Widespread use of pirated software- the most important challenge is preventing the cyber crime is the prevalence of software piracy, as pirated software is more prone to attacks by viruses, malware and Trojans.

COUNTERMEASURES FOR SECURING SECURITY ARCHITECTURE IN BANKS

Banks should tighten up their defence methods for safeguarding the data of customers and adopt countermeasures to make the banking system more immune to these attacks. In this section, we are attempting to suggest some countermeasures that banks should take up to mitigate the cyber security attacks and enhance the banking security infrastructure.[13]

- **Continuous Risk Assessment**

No two banks are alike. Each financial company has its own risk profile depending on its size, geographical setup, business operating sector, etc. Each company should perform a series of steps to put into effect security controls, identify threats, loopholes, risks and design and implement security controls that address these risks.

- **Countermeasures for Key Logging**

In order to protect keyboard input values, every portion of the entire system needs to be protected and this protection starts from the end user's keyboard inputting to what is saved in the memory of the web browser and finally what is reported on the user's screen. In order to provide keyboard security, everything needs to be detected in both the kernel level key logging and the user level key logging.

- **Countermeasures against Web Browser Attacks**

The web browser is the commonest target of most of the attackers. For safe online banking, we need a web browser technology that is able to protect itself against reverse engineering and debugging by attackers and should be able to block any attempt to access or modify its memory. It should obstruct COM (Component Object Model) Hooking and Cross Site Scripting as well as screen capture to prevent inputting the image type password. By falsifying host files or DNS, it should hinder Phishing attacks.

USER AWARENESS PROGRAMS:

[13] Beckett, A., Hewer, P., & Howcroft, B., "An exposition of consumer behaviour in the financial services industry". The International Journal of Bank Marketing, 18(1), 2000.

User is the key of any field and in some cases may be the weakest link in the chain. A bank can employ the latest security technologies but all are a waste if the customer does not know how to use them. Banks should frequently run some user awareness program for end users to inform them about the latest security features introduced by bank and how the customers can use them to secure their accounts.

CONCLUSION:

In India, the cyber crimes are rising significantly. The offences committed in the social media, credit card fraud, phishing, and virus, Malware, Denial of services, Gambling, Hacktivist, Personal data breach, corporate data breach and virtual currency are repeatedly done by cyber criminals. Involvement of males in committing cyber crimes is more in the age group 18-30 compared to females. The 60 and above age groups persons are also involved in cyber crimes. It is not good sign that senior citizens are also involved in cyber crimes. In the State wise list of cyber crimes, Maharashtra is at the top position. Most of the cyber crimes committed involve Nationalized Banks. The internet is the medium for huge information and medium of communication around the world, it is necessary to take certain precautions while operating it. With advancements in technology around the world, banks should not be left behind in terms of security systems; a sharp eye should be kept on vulnerabilities present in banking networks and emerging tricks and techniques used by hackers to bypass banking security and launch attacks. Tight security architecture should be implemented to provide a safe banking environment to users.

AN APPRAISAL ON BANKER-CUSTOMER RELATIONSHIP WITH SPECIAL REFERENCE TO RIGHT TO PRIVACY

Dr. G.Subhalakshmi*
&
Aparna B Sundar**

Abstract

Money, a medium of exchange, is an indispensable need for every individual in the present day situation; with which one can procure his personal requirements, food, shelter, property and can actually fulfill all his desires in the truest sense. Money also gives a status to man. Thereby, man looks for all possible ways and means to protect and preserve his money and this led to the launching of financial institutions like the Banks. Thus, the banks were considered as the saviors, and safe keepers of money. In the current day scenario, it is essential to maintain a bank account and the Government has also been insisting on the same in order to dole out the subsidies to every household. Opening a bank account creates an involuntary relationship between the banker and the customer and different types of services are availed by the customer. The bond between the two is multi-dimensional depending on the services rendered or availed, products sold or taken possession and so on. Therefore, depending on such services one can determine what relationship subsists between the Banker and Customer. Whatever be the type of contractual relationship, it shall impose certain rights and duties on such contractual parties and this extends and applies in the case of banking relationship too. The advent of Aadhar era and linking of the same with the bank account has made their relation even more crucial. Thus, this paper intends to enumerate the varied relationships that exist between the banker-customer while defining banker, customer and discussing about the nature of banking. The paper further details on the rights and duties of Banker and Customer, the confidentiality and the impact of right to privacy.

* Faculty, School of Law, Pondicherry University.
** School of Law, Pondicherry University.

Introduction

Money is not only important for man to have his needs met but also gives him a social status. Thereby, man looks for all possible ways and means to protect and preserve his money and this lead to the launching of financial institutions like Banks. The banking system is said to have originated even before 2000 B.C in Babylonia through the activities of temples, which were preferred places for safekeeping of valuables like grains, agricultural tools, and precious metals etc. The receipts issued by the temples came to be used for transfer of the stored items to third parties. Thus banks started as safe keepers and evolved into institutions by offering fund transfer facility and later credit facilities.[1]

Scope and Objective

In the current day scenario, it is essential to maintain a bank account and the Government has also been insisting on the same in order to dole out the subsidies to every household. Almost every citizen has an account with the bank. Opening a bank account creates an involuntary relationship between the banker and the customer and different types of services are availed by the customer. Customers open accounts with the bank on the basis of trust that they have with the bank. Maintaining a level of trust is thus very essential for the smooth functioning of the banking system. With the changes introduced in the society and the advent of the Aadhaar Card, this relationship is becoming crucial and there exists a threat too. Thus, this paper intends to enumerate the varied relationships that exist between the banker and customer about the nature of banking. The focal point of the paper would be on the rights and duties of Banker and Customer, the confidentiality and its impact on right to privacy. Further, the work is guided by the following objectives:

- To study and understand the evolution of Banking system.
- To understand and discuss the different roles played by the Banker, the right and duties of both the Banker and Customer.

[1] M.N Gopinath, " Banking Principles and Operations", Snow White Publications Pvt. Ltd, Mumbai , Fifth Ed, 2014, p.5

- To identify the significance, relevance and importance of the Banker-Customer relation and confidentiality between them.
- To bring to light the deficiencies of the present system and the suspicion arising with regard to right to privacy of the Customer.

Research Questions

1. To what extent the linking of Aadhar card to the Bank account impact the Trust-bond between the Banker-Customer?
2. How does the linking of Aadhar card to Bank account affect 'Right to Privacy'?

Methodology

The methodology adopted in this study is doctrinal, descriptive and analytical. It is basically a theoretical work which is built up from the information gathered from books, journals, government portals and government and non-government reports. Internet has been a key source in collecting the views and opinions of various eminent writers. Adapting the method of doctrinal research, legal concepts and principles have been examined and analyzed to reach the conclusion. Daily Newspapers and magazines are also used as valuable information for the study.

Genesis of Banking System

In England, during the reign of King Edward III, money changing was an important function of bankers which was taken up by the Royal Exchanger, for the benefit of the Crown. He exchanged the foreign coins tendered by the travelers into British money and on the other hand, he supplied persons going out of the country with the foreign currency required. Thus, it can be said that the ground of modern banking was laid during the reign of Queen Elizabeth I, on the influx of gold from America. The city merchants decided to keep their cash with goldsmiths. Thus, large sums of money were left with the goldsmiths, for safe custody against their signed receipts known as "gold smith's notes" which formed the foundation of "issue" and "deposit" banking.[2]

[2] R.N Chaudhary, "Banking Laws", Central Law Publications, Allahabad, Second Edition 2012, p.15

The Bank of England Act, 1694 which is otherwise called t*he Tonnage Act* was passed, by which the Governor and company of the Bank of England was incorporated. *The Peels Act, 1884* gave new dimensions to banking because greater attention began to be paid towards deposit banking and cheque currency.[3]In the present day scenario, almost every individual has an account with the bank as it has become indispensable in our day to day lives. The evolution of Banking can be broadly studied under two divisions viz., early banking and modern banking system.

"*A bank is basically a financial institution licensed to receive deposits and make loans. Banks may also provide financial services, such as wealth management, currency exchange and safe deposit boxes. In most countries, banks are regulated by the National Government or Central Bank.*"[4]

With the above definition of bank, a question arises as to whether the Banking Regulation Act, 1949, defines the term 'Bank'? The answer to this Question is No. because the Banking Regulation Act, 1949 does not define the term Bank. It is also safe to say that the term **'Bank'** has not been defined by any of the Indian Legislative Acts. However, the term 'banking' has been defined under section 5, clause b of the Act as; *"banking means accepting, for the purpose of lending or investment, of deposits of money from the public, repayable on demand or otherwise, and withdrawal by cheque, draft, order or otherwise."*[5] To wrap up, a bank can be defined as any financial institution that accepts money from the public, for the purpose of lending or investments.

Review of Literature

(i) K.P.M Sundharan and P.N Varshney (2009), deal with the theory of Banking and Indian banking, and explain the structure and the functions of Reserve Bank of India as well as Commercial Banks.[6]

(ii) Kamalendu Bhattacharya and Samir Kumar Basu (2010), deal specifically with bank suits and handling of security documents.

[3] *Ibid*
[4] Retrieved from www.investopedia.com last accessed on 10/12/2018
[5] S. 5(b), Banking Regulation Act, 1949.
[6] K.P.M Sundharan and P.N Varshney, "Banking Theory Law and Practises", Sultan Chandra & Sons, 18th Ed 2009.

The book has been written with the aim of instilling a high degree of confidence among bank officials when it comes to handling the confidentiality of its customers.[7]

(iii) R.N. Chaudhary (2009) in his book emphasizes that there is no other fundamental change except for the power and functions of the Reserve Bank under the Banking Regulation Act.[8]

(iv) Jyoti Panday (2017), specifically talks about the *Puttaswamy case* and how this case brought about a shift on how "right to privacy" is construed especially in light of linking Aadhaar Card.[9]

(v) Anurag Bhaskar (2017) in his commentary entitled *"Key Highlights of Justice Chandrachud's Judgment in the Right to Privacy Case" (27/AUG/2017)* talks in detail about the judgment delivered by Justice. D.Y Chandrachud on Right to Privacy. The author links the judgment to Aadhaar with the following words of the Judgment *"….. the right to scrutinize and the right to dissent which enables an informed citizenry to scrutinize the actions of the government."*

(vi) *The Economic Times*, in its article entitled *"View: Have no fear, Aadhaar is linked to logic"* dated Feb. 13, 2018; states that the Government of India wants its citizens to link Aadhaar Card to their Bank Accounts mainly so as to be able to provide some form of information when it comes to the disclosure of their income. This article had also suggested that, "this could also be the backbone in case a decision is taken on the universal basic income scheme." Moreover linking of Aadhaar Card to accounts could be used to deliver benefits such as comprehensive social security.

Banker

Banking is a business carried on by the bankers/banks. A banker is "an individual that is employed by a banking institution and participates in various financial transactions, which may or may not include investments". There is no specific provision in the Banking Regulation Act or any other Act dealing with 'banker'. But the following

[7] "Bank Documentation and Correspondence" published by Kamal Law House, Kolkata (2010)
[8] R.N. Chaudhary (2009) with the book "Banking Laws" published by Central Law Publications, Second Edition.
[9] Jyoti Panday (2017), in "*India's Supreme Court Upholds Right to Privacy as a Fundamental Right – and It's About Time*"

Acts can help us define 'Banker' under the Indian Law. (i) ***Section 3 of the Negotiable Instruments Act, 1881***: "Banker" includes any person acting as a banker and any post office savings bank. (ii) The term 'person' has been widely defined in the General Clauses Act, 1987. Accordingly, it includes individual or body of individuals or association whether incorporated or not. ***Section 11 of the Companies Act, 1956*** Section 11 (2) declares that no company, association or partnership consisting of more than twenty person (ten in case of banking business) shall be formed for the purpose of carrying on any business that has for its object the acquisition of gain for itself or for its members unless it is registered as a company under the Companies Act or is formed in pursuance of some other Indian law. Therefore it is obvious by this provision that banking business may be carried on by a group of individuals provided that number of persons is limited to ten and not more than that. In 1931, provisions relating to banking business were made separately, and in 1949 Indian Banking Companies Act were passed which is named as the ***Banking Regulation Act in 1949***.[10]

The Banking Regulation Act, 1949 Section 5, Clause b, Section 5, Clause (c) and Section 7 of the Act are relevant in defining 'banker'. Section 5(b) states "banking"; Section 5(c) "banking company" and Section 7 states the use of words "bank, banker, banking". No company other than a banking company shall use as a part of its name or in connection with its business any use of the words "bank", "banker" and "banking" and no company shall carry on the business of banking in India unless it uses as part of its name at least one of such words. This section also prohibits use of these words by any firm, individuals or group of individuals. To sum up, "Bank", "Banker" or "Banking" words are *sine qua non* for banking business by a banking company. It is therefore clear that banking business can be carried on only by banking companies. No individual or group of individuals or firm can carry on banking business, though they can carry on money lending business. Money lending business is different from banking business.[11]

Customer

[10] https://www.investopedia.com/insights/what-is-money/ last accessed on 13/12/2018
[11] Retrieved from http://www.businessdictionary.com last accessed on 13/12/2018.

There is no statutory definition of a customer in the Indian statutes, but banks appear to rely upon certain facts to recognize a customer; For a person to be known as a customer of the bank, he must either have a current account or any sort of deposit account like saving, term deposit, recurring deposit, a loan account or some similar relation. The word 'customer' signifies a relationship in which duration is not of essence. A person whose money has been accepted by the banker on the footing that he undertakes to honour cheques unto the amount standing to his credit is a customer of the bank irrespective of whether his connection is short or long duration. There are different kinds of customers like Individuals, Joint Hindu Family (JHF), Partnership firms, Joint stock companies (Limited Liability Companies), Clubs, Societies and Associations, Trust Account.[12]

Banker-Customer Relation

The relationship between the banker-customer can be said to be multi-dimensional depending on the services rendered or availed, products sold or taken possession and so on. Therefore, depending on such services one can determine what relationship subsists between the Banker and Customer. The general relationship between banker and a customer is that of a relationship of a debtor and a creditor. When the customer has a credit balance in his account, the customer is the creditor and the banker is the debtor. Conversely, where the customer has a debit balance in his account, the customer is the debtor and the banker the customer.[13] When securities and valuables are deposited for safe custody, the banker assumes the role of a trustee and the customer still continues to be the owner of the goods. A trustee is one who holds property for the benefit of beneficiary and the profits accruing from those properties belong not to the trustee but to the beneficiary. So, a banker, who uses the money in a manner he likes and is entitled to pocket whatever profits he makes cannot be called as a trustee of the customer's money.[14]

When the customer leaves with the banker some valuables for safe custody in deposits, vaults or lockers, the banker performs the role

[12] *Ibid*
[13] Dr S. Guruswamy, "Banking Theory Law and Practice", McGraw Hill Education, Uttar Pradesh, 2008, p.209
[14] S.S Gulshan and Gulshan K.Kapoor, "Banking Law and Practice", S. Chand & Co Ltd, 1994, p.75

of a bailee and the relationship between the banker and the customer is that of a bailee and a bailor.[15] A banker also acts as an agent of his customer and performs a number of agency functions for the convenience of his customer viz., he buys and sells securities on behalf of his customer, collects cheques on his behalf and makes payment of various dues of his customer. When credit facility is provided by the bank to a customer against the security of immovable property, the relationship of Mortgagor and Mortgagee is established.[16] The customer of a bank takes loan from the bank by way of security of moveable property is called a "pawnor" (pledgee) and the relation between customer and banker stands Pawnor and Pawnee (Pledgee). Sometimes the relationship of a banker and customer also arises as lessor and lessee, where there is a transfer of interest relating to immovable property between the banker and its customer. When a customer hires a locker, the relationship between the parties is that of a lessor and a lessee.[17]

Rights and Obligations of the Banker

The rights available to a banker are Right to Lien, Right of Set-off, Right of Appropriation of payment, and right to charge interest. The Banker also has some crucial obligations towards his customer by the relation with his customer. Some of them are:

- Honoring of Cheque,
- Maintaining the secrecy of the Accounts of his Customer,
- Honoring Guarantee
- Honoring letters of credit
- Maintaining proper accounts of his customer
- Recovery of Debts

Rights and Obligations of the Customer

By opening of an account with the banker, there arise some rights and responsibilities on the customer. There are no specific statutory provisions but customers have such rights and duties by the

[15] Retrieved from http://www.gr8ambitionz.com last accessed on 13/12/2018
[16] Retrieved from https://indianmoney.com last accessed on 13/12/2018
[17] Supra Note1 p.127

relationship with the banker they have. The rights and obligation of the customers may be summarized as drawing cheques with reasonable care and not to draw without sufficient fund, to repay the over drawings and charges of the bank, to communicate facts and to make demand for repayment of deposits and so on.

Confidentiality between Banker and Customers

Under the Indian Law, the right to privacy is taken upon with much care. This protection is available in the banking system, especially when it comes to the relationship between banker and customer. It is expected that the banker does not divulge any information belonging to his customer to any third party. The banker is expected to maintain his customer's secrecy except for certain circumstances that is permitted by law. However, there are also certain conditions as to when the concept of confidentiality does not apply like the disclosures to be made if law mandates, if disclosure is permitted by the implied consent, and for bank's reference purpose.

Right to Privacy in an Aadhar Scenario

The right to privacy in India has developed through a series of judgments over the past 60 years. Over the years, inconsistency from two early judgments created a divergence of opinion on whether the right to privacy is a fundamental right. However, from the recent judgment delivered in Justice K.S. Puttaswamy (Retd) vs. Union of India, these inconsistencies have been removed. Moreover, in order to properly understand Right to Privacy, the constitutional provisions must be read and interpreted in a manner which would enhance their conformity with International Human Rights instruments ratified by India.

The judgment states the reason behind the one-page order spans 547 pages and includes opinions from six judges, creating a legal framework for privacy protections in India. These opinions cover a wide range of issues in clarifying that privacy is a fundamental inalienable right, intrinsic to human dignity and liberty. The decision is especially

timely given the rapid roll-out of Aadhaar. In fact, the privacy ruling arose from a pending challenge to India's biometric identity scheme[18].

Ambiguity on the nature and scope of privacy as a right in India allowed the Government to collect and compile both demographic and biometric data of residents in the name of Aadhar, a 12-digit unique identity number to each resident. It is on voluntary basis which is available to an individual permanently as it does not need renewal from time-to-time. The original justification for introducing Aadhaar was to ensure that government benefits reached the intended recipients. The government's push for Aadhaar has led to its wide acceptance as proof of identity, and as an instrument for restructuring and facilitating government services.[19]

It is the world's largest biometric ID system, with over 1.19 billion enrolled members as of 30 November 2017, representing over 99% of Indians. World Bank Chief Economist, *Paul Romer* described 'Aadhaar' as **"the most sophisticated ID programme in the world".** It is considered a proof of residence and not a proof of citizenship. Aadhaar does not itself grant any rights to domicile in India. In June, 2017, the Home Ministry clarified that, Aadhaar is not a valid identification document for Indians travelling to Nepal and Bhutan.[20]

(Justice K.S. Puttaswamy (Retd.) v. Union of India)

The Right to Privacy in India has also been an ambiguous subject. Before the pronouncement of this judgment, citizens did not enjoy their 'right to privacy'. Privacy was always considered a privilege rather than a right. With the advent of the Aadhar Card, the constitutional validity of this right was about to change. It is important to bear in mind that the nine-judge bench that was formulated was not set up to look into the constitutional validity of the Aadhar, but to look into the

[18] Retrieved from www.eff.org "India's Supreme Court upholds Right to Privacy as a Fundamental Right- And it's about time." By Joyti Panday last accessed on 15/12/2018.
[19] *Ibid*
[20] Supra Note 1

constitutional validity of the 'Right to Privacy'. The Aadhaar Card functioned as a catalyst to speed up the process in granting the Indian citizens '*Right to Privacy'*.

The nine-judge bench of the Supreme Court has unanimously delivered its judgment in ***Justice K.S. Puttaswamy (Retd.) v. Union of India***[21] holding that privacy is a constitutionally protected right which not only emerges from the guarantee of life and personal liberty in Article 21 of the constitution, but also arises in varying contexts from the other facets of freedom and dignity recognised and guaranteed by the fundamental rights contained in Part III of the Indian constitution.[22]

The bench over-ruled the decisions given in the cases of *M.P. Sharma v Satish Chandra, District Magistrate* (1954) rendered by eight judges, and *Kharak Singh v State of Uttar Pradesh* (1962) rendered by six judges, stating that right to privacy is not a fundamental right and that the Indian Constitution does not specify a separate protection for such right. Upon reviewing the judgment given by the nine-judge bench of the Supreme Court, it is clearly seen that the scope of 'right to privacy' as a fundamental right has brought about a lot of scope within the right itself. This judgment has brought about an awakening in the country whereby people are now more empowered to lead a dignified life and to question authorities whenever they feel certain duties are imposed on them causing the infringement in their privacy. With the pronouncement of this judgment, making privacy a fundamental right; a new light is shed on the Aadhaar Card. The Indian Government demands that the Citizens must link their Card to their Bank Accounts. Many are of the view that linking of the card with their account number will only result in the loss of their privacy. With the presence of this judgment the masses are now empowered to fight back and protect their privacy. This judgment paved a new form of empowerment for its masses.

Eventually, the Supreme Court on September 2018 had finally upheld the validity of Aadhaar but at the same time has struck down

[21] Writ Petition (civil) no. 494 of 2012, Supreme Court of India.

[22] Retrieved from https://thewire.in "Key Highlights of Justice Chandrachud's Judgment in the Right to Privacy Case." By Anurag Bhaskar last accessed on 15/12/2018

some provisions like the linking of Aadhar with the bank account and mobile phones. Further, the Court dismissed the apprehension that the Aadhaar Scheme violates 'right to privacy' as only minimal biometric data was collected from the citizens for the process.

Conclusion:

Banks have always taken pride in their ability to serve their customers. A majority of such customers have been family customers, meaning that their family wealth has been entrusted in these banks for generations and more generations to come. When these individuals have been long term customers of the bank, a bond is automatically established between them, which leads to the establishment of the Confidentiality Agreement between Bankers and Customers. The word "confidentiality" and "privacy" are somewhat synonymous. Confidentiality involves a sense of 'expressed' or 'implied' basis of an independent equitable principle of confidence. Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others.

Moreover, the Information Technology Act, 2000, is not equipped with handling the prevention of leak of data especially from something as massive as the Aadhaar. This Act is not a data and privacy legislation **per se.** It has not laid down any specific data protection or privacy principles. We can say that the Act is basically a generic Act. If the protection of the data collected for Aadhaar is the first priority of the Government, then the Government needs to reframe the Information Technology Act.

IMPACT OF TECHNOLOGY IN BANKING

R. Aswini Ramesh*

ABSTRACT

The revolution of applications is fundamentally impacting the most regulated industry in the world – Banking. The current era is all about the positive influence of technology on the banking industry. People prefer to perform their banking activities without entering the bank premises by using their smart phones to interact and invest with their banks. Mobile technology offers new opportunities to banks to provide additional convenience to their customers and reach the large population of unbanked customers. Mobile banking apps are nowadays becoming the need of the consumers, providing them contextual information in a highly convenient and personalized manner. There is not a single industry in the world that is not experiencing the impact of smart applications, the banking sector too has been transformed by them and is ushering in a new era of innovation. There are rapid changes in the way banking sector is operating due to the proliferation of mobile devices and applications. Over the last few years, banking apps have been steadily gaining greater popularity with consumers, thus enabling banks to offer improved products and services, all the while streamlining their operations and exploring new opportunities to cross-sell and up-sell banking services and to expand into other markets to increase revenues.

While some banking consumers still prefer traditional banking practices like visiting the local branches, the reality is that most of them are now demanding the ability to access essential banking services and options while on the move employing a mobile device. Therefore, it has become imperative on the part of banks to provide a secure and reliable platform for their financial transactions. This paper is an attempt to study the advantages, vulnerabilities, reliability and various other issues connected with the usage of this modern banking tool.

Introduction

Advancement in technology has changed the way we seek information, communicate with family and friends, create new opportunities and relate to

* III year, SOEL.

our Banks. Banking has certainly come a long way since its birth in the goldsmiths' shops[1] of 17th century London. Times have changed, and today's digital world is having wide spread effects on an array of consumer behaviors, where electronics and mobility have become key trends for the financial institutions and changed the way we handle our finances. Banking apps via smart phones or tablets are coming on strong in many countries, with enormous potential to satisfy the never-ending demands of the customers. Mobile banking started in India in 2002, and transactions were carried out through SMS. Today with the help of mobile banking apps, almost all banking transactions like electronic bill payments, remote check deposits, P2P payments, fund transfers, open and close fixed and recurring deposits and scheduling transactions can be carried out as per the customers' convenience. The popularity of the smart phone has lead to the inevitable rise in digital banking via various smart phone apps, with more and more people increasingly using apps to access a broader range of banking services.

The introduction of mobile banking in the 1980's helped banking industry to achieve exponential growth in the increased mobile transactions and improved customer service. 'Digital India' a government initiative launched in 2015 to improve internet connectivity, digital literacy and the nations technology infrastructure, aims to increase participation in the digital economy, through mobile banking platforms, cashless transactions, increased awareness of these services and thus improve financial inclusion. Cashless transactions are growing fast in our society. Different banking methods are used in various sectors of our society. This paper is an attempt to assess the evolution of modern banking apps, the omnipresent risks of the technology, awareness and preparedness, regulatory and supervisory issues as set forth in the RBI Guidelines.

Modern Banking:

Since Nationalization of Banks in 1969, the Indian Banking has come a long way from being a sleepy business institution to a highly proactive and dynamic entity. Banks have come up with a plethora of exciting and innovative applications for their consumers to access their accounts anytime and anywhere. Any successful banking application needs simplicity, contextuality, engagement and security.

[1] https://www.rbs.com/heritage/rbs-history-in-100-objects/history-in-100-themes/going-the-extra-mile/banking-app-2011.html

Some of the innovative mobile payment apps include :

Digital Wallets:

A digital wallet is a software-based system for making e-commerce transactions which can be done using computers, smartphones or tablets. It has two major components, namely, software application and information storage. The software application is responsible for security, actual transaction and encryption which provides user interface as well. The user information stores data base such as billing and shipping address and payment methods. Merchants benefit because they are protected against fraud and they sell more products faster. A smart phone digital wallet also helps one to store concert tickets, bus and subway passes and gift cards. A digital wallet could alter the way one organizes one's finances and life in general.[2]

Mobile commerce apps:

Mobile commerce (m-commerce) is the use of wireless hand-held devices such as mobiles and tablets to conduct online commercial transactions. Computer mediated networks enable these transaction processes through electronic store searches and electronic point of sale capabilities[3]. The range of platforms that are enabled for mobile commerce functionality is growing. Social media platforms like Facebook, Instagram, Twitter and Pinterest launched "buy buttons" on their mobile platforms in the mid-2010's letting users conveniently make purchases from other retailers directly from the social media sites. Digital wallets like Apple Pay and Android Pay allow customers to seamlessly make purchases without swiping cards at stores or via mobile commerce application. Goods and services that are applicable under m-commerce so far include mobile money transfer, mobile ATM, mobile banking, mobile vouchers, location-based services, mobile ticketing etc.

Person-to-Person Payment Platforms:

Person-to-person payments (P2P) are an online technology that allows customers to transfer funds from their bank account or credit card to another individual's accounts via a mobile phone or the internet. P2P payments can be initiated using two different methods. In the first method, customers use a mobile application or an online interface developed by the bank or financial institution to designate the amount of funds to be transferred to recipient

[2]https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/digital-wallet.htm
[3]https://www.techopedia.com/definition/1540/mobile-e-commerce-m-commerce

whose email address or phone number is designated. The recipient uses the online interface to input his bank account information and routing number to accept the transfer of funds. The second method is based on the successful Paypal approach where their bank account or credit card information is designated with a trusted third-party vendor for transfer and acceptance of funds. Users can complete the process of receiving or sending funds using the third party's mobile application or website. The most appealing benefit of P2P transfers is cost, transparent pricing and security. All transactions happen electronically with the system automatically matching buyers and sellers without a middle man, thus enabling low transaction fees ranging from 0-1%. Currency conversions are publically listed and the exact rate is determined solely by supply and demand and not by governments or banks. Very little personal identity information is attached to a transaction, thus preventing data breaches. As commerce evolves beyond the individual to merchant relationship to a broader individual to individual exchange, banks and financial institutions are finally getting in on the action.

Unified Payments Inferface (UPI):

It was created by the National Payments Corporation of India (NPCI) set up by the RBI and Indian Bank's Association (IBA). UPI is a unique payment solution which enables faster, easier and smoother instant online payment of utility bills, school fees, over-the-counter payments, taking customers to the virtual world of new age banking landscape. All the customer needs is a smart phone with a UPI app downloaded which does all the functions of a debit card or internet banking in a more secured environment. When a customer downloads the UPI app of a bank, UPI facilitates 'virtual address' as a payment identifier for sending and collecting money and works on single click two-factor authentication. It also provides option for scheduling push and pull transactions for various purposes like sharing bills among peers. UPI enables instant and secure P2P transactions with a simple user experience[4]. It provides for a great and enabling foundation for Fintech companies to provide innovative user experiences, tools and services to all these customers including the low and moderate income customers, who haven't had access to the best of product, pricing and the user experience of the growing number of PMJDY accounts.

DISTRIBUTED LEDGER TECHNOLOGY (DLT)

[4]https://indianexpress.com/article/technology/tech-news-technology/unified-payments-interface-upi-payment-system-faster-easier-and-smoother-2754125/

It is a digital system that can record transactions spread across multiple sites, countries or institutions with faster processing, reduced cost and security at the same time without a central administrator or a centralized data storage. A DLT database combines shared data bases and cryptography and allows several entities to access an immutable digital ledger simultaneously. A DLT database is held and updated independently by each participant in an extensive network, distribution is unique because a central authority does not communicate records to various nodes. Files are independently constructed and held by every node. Each node on the network processes every transaction, comes to its conclusions and then votes on those conclusions to ensure majority agreement. Once consensus is reached, the distributed ledger is updated and all nodes maintain an identical copy of the ledger[5]. DLT addresses several banking pain-points by providing increased transparency and tamper proof transactions in real time. Thanks to the cryptographic protection offered by DLT, banks are also exploring use cases in digital identity and KYC by setting up a shared digital utility to record identities.

BANKING APPS – A RAGE

Over the past decade, banks globally had been embracing innovation at a staggering pace to enhance many of its customer facing and front-end operations to come up with diversified banking solutions across multiple digital channels such as internet, mobile, social media, 24/7 electronic branch, digital wallet etc., providing customers with an unparalleled banking experience. Here we will have a look into the major benefits of technological advancements in banking applications.

- **Business Efficiency** – Improves interaction with customers and delivers their needs efficiently and quickly[6].

- **Improved Accuracy** – Financial accuracy is crucial for banks to comply with government regulations. Paper processing may have an error rate of up to 40% requiring reworking. Simplifying verification processes it becomes easier to implement IT solutions with business software leading to accurate accounting.

[5] https://www.capgemini.com/2018/08/more-and-more-banks-are-investing-in-distributed-ledger-technology/
[6] https://genbin.genesys.com/old/resources/success-stories-and-infographics/Genesys_Case_Study_-_TXU.pdf

- **Improved Competitiveness** – Banks find it easy to reach broader markets and build closer relationship with tech savvy consumers due to the innovations in banking applications.

- **Cost Cutting** – By simplifying products, services and underlying processes banks can realize spectacular operational cost savings and aim to have a back office with no employees. The savings can be passed on to the customers in the form of lower fees, higher yields and more generous account thresholds.

- **Eco-friendly** – There will be no paper statements, no errands driving to the bank and no additional space needs for staffing or housing of operations.

Banks coming up with several advanced apps and banking options help customers do banking from anywhere and at anytime efficiently and safely. With a few clicks on their mobile devices, money can be transferred and bills can be paid. Many businesses have built their brands and are thriving, every process is made simple, instant decisions can be made and errors and delays can be quickly sorted out, with a positive impact on productivity. Loan calculators, premium calculators, financial planning tools, investments, budgeting, forecasting, tax preparation are some of the sturdy features offered to customers helping them in financial planning without the need to personally visit a bank. Time management is crucial for a successful business and precious time is saved by these utilities offered by the banks.

Disadvantage:

Below are some of the key disadvantages of app-based banking transactions. (i) The first and foremost concern about any app-based transaction is the security issues. Users always are under the fear of identity theft and misuse of their money by hackers and frauds. (ii) Enough support infrastructure, financial inclusion, literacy and dispute resolution processes are not sufficient in countries like India where people are backward in their technological growth and always stick to age old thinking and lifestyle. (iii) Another big problem that we face is that in every-day life, we are unable to pay small value money using these apps. In the case of P2P payments refunds are non-existent and difficult to dispute charges after the fact. (iv) Speculation and unpredictability is another downside. Currencies like Bitcoin can easily be

converted to Dollars, Euros or Yen but there is no guarantee that you will recoup the original value of transaction you initiated with the P2P currency.

Vulnerabilities

Banking has gone digital. Every bank in the country offers an online portal or a mobile app and people seem to prefer it that way. Users crave the convenience that comes with banking on the go, but the undeniable question of security of these banking apps still persists. Some noticeable trends in banking industry from the security point of view may be discussed here.

A few technological blights in digital banking in India are Cracking, E-mail and SMS spoofing, Carding, Intellectual property Crimes, Financial crimes, URL Hijacking, Virus transmission, Hacking, Cyber terrorism etc.,[7]

- Compared to other industries cyber-attacks are said to be three times higher in the financial sector.

- Managing regulatory compliances has become enormously challenging for the banks[8].

- Next generation ransomewares, web attacks etc., are due to the huge technological developments in the industry.

- The cost of managing and implementing cyber security infrastructure is estimated to increase over 40% by 2025.

- Financially savvy criminals monetize stolen identity data obtained from corporate data breaches.

[7] www.iosrjournals.org/iosr-jbm/papers/conf.17037-2017/volume-8/10.%2055-62.pdf
[8] https://www.bdo.in/getmedia/b478e1ec-a9a3-4afe-997a-3aed7d190164/Cyber-Security-in-banking-industry.pdf.aspx?ext=.pdf&disposition=attachment

- According to the 2018 cyber-crime reports, there were 210 million cyber-attacks world -wide within the first three months of the year.

- Cross border transactions are said to be 5.4 times more likely to be fraudulent than those made domestically.

- The growing pool of consumers and businesses seeking access to goods and services globally is also worsening the problem.

- In developing countries with large number of unbanked and under banked customers, there is a rapid increase in people managing their entire financial lives on mobile devices. Due to lack of familiarity with fraud risks, they easily fall prey to social engineering attacks.

- With the increase in P2P mobile payment platforms there is a parallel increase in cyber-crime.

- The world bank group's computer network one of the largest repositories of sensitive data about the economies of every nation has been raided repeatedly by outsiders[9].

- E-commerce web applications were most exposed to denial-of-service attacks which results in downtime in their online operations[10].

- In December 2017, several popular banking apps were found vulnerable to man-in-the-middle attacks that can let hackers snoop around their traffic and steal banking credentials.

- The most common online bank vulnerabilities in 2017 are cross-site scripting (75% of systems) and poor protection from data interception allowing attacks such as reading cookie values or stealing consumer credentials.

[9] https://www.infowars.com/world-bank-under-cyber-siege-in-unprecedented-crisis/
[10] https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/vulnerabilities-in-banking-related-web-applications-highlight-significance-of-secure-devops

- In Mobile banking apps, attackers could exploit vulnerabilities to decrypt, intercept or brute force accounts to access the mobile app or bypass authentication.

- On average, IOS apps are better protected than android, even when created by the same bank where it accounted only 25% of total vulnerabilities compared to 56% on android.

- Financial products have multiple data interfaces with other service applications and most of the products have multiple application program interface. These API's are exposed to untested/untrusted interfaces leading to compromise of security measures[11].

- Several incidents related to debit card security compromise were attributed to security attack on third party service provider.

CYBER ATTACKS IN INDIA

In August 2017, Cosmos Corporative Bank Ltd witnessed a massive security breach when hackers siphoned of around Rs.94 Crores through a malware attack on its server. In the same year, City Union Bank came under attack after cyber criminals transferred nearly $2 million via the swift to unauthorized lenders overseas. On July 2018, fraudsters hacked into Canara Bank ATM servers and wiped off almost Rs.20 lakhs from different bank accounts[12]. As per the information presented by the CERT, over 493 websites were affected by the malware propagation. Recently in August 2018, around Rs.4 crore was transferred illegally through sim card swap fraud.

Stay Alert. Stay Ahead

The public sector banks have seen an explosive growth in the use of personal computing devices, internet connectivity and innovative products. In trying to making their processes more efficient, banks are resorting to outsourcing, quicker development, deployment, cycle of products, services, processes, keeping in view cost, convenience, profitability and consumer satisfaction. Due emphasis in security, design and testing is ignored in the

[11] https://assets.kpmg.com/content/dam/kpmg/in/pdf/2017/04/Digital_payments_Analying_the_cyber_landscape.pdf
[12] https://www.testbytes.net/blog/cyber-attacks-on-india-2018/

hurry leaving loop holes for attackers to exploit. Here are some ideas that could protect the banks becoming targets of economic terrorism.

Customer Data Protection

As custodians of customers data, banks are responsible for its preservation, confidentiality, and availability irrespective of whether the data is stored/in transit within themselves or with customers or with the third-party vendors. Suitable systems and procedures need to be put in place to safe guard the same.

Better risk assessment

Risk mitigation strategies should be developed to assess attributes such as customer type, volume and capability of transaction methods, security and sensitivity of information, financial loss, liability, corporate risk and reputational damage, in reasonable intervals of time.

Strong Authentication Standards

Simple Usernames and passwords and traditional two-factor authentication solutions are no longer effective against sophisticated man-in-the-middle browser attacks Strong authentication, out-of-band transaction verification, mobile authentication and extended validation, SSL digital certificates and biometric authentication, provide better protection of transactions and customer identities

Security and network management

Individual security operation centers to monitor adherence to Standard Operating Procedures in all major IT activities with the help of a security incident and event management system. The status of patches to operating system and application software running at end-user devices directly connected to the internet and in respect of server operating systems/data bases/applications/ middleware should be monitored.

Enhanced customer awareness and Education

Customers should be educated to protect and mitigate cyber threats. Customers should be encouraged to monitor their accounts on regular basis

to track for unauthorized transactions, avoid sharing personal information over email, call or on pop-up windows, use strong unique passwords etc.,

Knowledge is power

A vast majority of malware proliferates through a series of online social engineering schemes that manipulate unsuspecting users to open the door wide for hackers. The employees themselves, as the first line of defence should learn how to spot phishing schemes, identification techniques, security practices (using password managers, logging out of devices before leaving them unattended etc) to significantly reduce the risk of user driven compromise.

Monitoring Threat

Majority of data breaches are furtive in nature, the sooner one detects an indicator of compromise, the sooner one should take action to prevent harm to a financial institution. The significance of real time threat monitoring is notable.

Forensic Technology

The technologies and processes for detecting and preventing cyber threats have been evolving side by side with the strategies of fraudsters using new and sophisticated methods of attack. Cyber forensic experts can adequately identify, collect and preserve evidences such as hard disk, mobile phone images, fire wall, appliance logs, server/desktop logs in a forensically sound manner. Cyber forensics can be increasingly leveraged to detect cyber crimes.[13]

CONCLUSION:

The dependence on technology is such that banking business cannot be taught of in isolation without technology in the Indian commercial banking landscape Customers are rapidly adopting technology in their daily lives driven by the growth in internet and mobile penetration, availability of low-cost data plans and shift from offline to online commerce. Banks in India are encouraging the development of a whole ecosystem of digital banking products

[13]https://assets.kpmg.com/content/dam/kpmg/in/pdf/2017/04/Digital_payments_Analying_the_cyber_landscape.pdf

and services using digital technologies to provide faster and convenient service to all segments of the rural and urban markets[14].

Regulators are responding to challenges posed by technological innovation and are seeking to strike a balance between mitigating the potential risk associated with this development and not impeding the positive effects of innovation. A robust regulatory framework, an effective customer redressal framework, fool proof security measures to enable confidence and trust are some measures that can help ensure long term success for the digital eco system. Banking is no longer just apps, websites or physical branches. Going to bank, a routine business core, will soon become part of history and so will the long queues, vouchers, pins and blue stamps.

[14]https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WGFR68AA1890D7334D8F8F72CC2399A27F4A.PDF

Section-II

e-Banking and related issues

BURGEONING FACILITY OF e-BANKING - AN ANALYSIS

Monisha. D*

ABSTRACT

Liberalization, Privatisation and Globalisation have brought forth many technological improvements in order to enrich the economical growth of a country. E-Banking is one of such aspect which came into being through various banking reforms in order to make the process of banking easy and effective. E-banking facility was provided first by private sector banks which was later adopted by the public sector and other banks. In order to regulate the facility of internet banking services certain legislations were laid down in the form of Amendments to RBI Act, 1934 and Banking Regulation Act, 1949. Certain recommendations of "Working Group of Internet Banking" committee were adopted as a result of which Information Technology Act, 2000 was amended in 2008 to provide for stronger data protection by punishing offences related to e-banking. However while relying on these amended provisions whether there is any lacuna in the service of internet banking is a question to be considered. The author in this paper will deal with questions regarding is the difference between traditional banking and e-banking ; whether e-banking facility is an improvised one; whether this facility is certain and can be assessed by all kinds of consumers; What percentage has it contributed to the digitization of a developing country in what ways the cyber crimes and protection of consumers' data are addressed etc.

INTRODUCTION:

E-Banking or Internet 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.[1] It is nothing more than a traditional banking services delivered through an electronic

* B.A.L.L.B (HONS), IV Year, School of Excellence in Law.

[1] Shilpan Dinesh Kumar Vyas, Impact of E-Banking on Traditional Banking Services, Research Gate (Dec.16, 2018). https://www.researchgate.net/publication/258726999-Impact-of-E-Banking-on-Traditional-Banking-Services.

communication backbone, viz, the internet.[2] For this, customer of a financial institution must be a registered user with a password for authentication. With the advancement of technology, India witnessed the emergence of e-banking after the economic reforms of 1991. Later the consumers started having nexus with e-banking facility rather the traditional banking which seemed to be time-consuming. The entire system of e-banking proved to be swift and convenient and has shown a great deal of resilience. This technology was first adopted by private and foreign sector banks and in turn created a pressure over public sector banks to compete equally on par with them in order to increase the consumer base. Although e-banking technology has improved the banking system and contributed to the economic growth of a country, it posed a threat of security to the privacy of the consumers from cyber frauds. So to address the issues arising from information security certain provisions and amendments were made to adopt and control the process of e-banking on legal perspective which will be discussed further.

DEFINITIONS:

Internet banking refers to the deployment over the Internet of retail and wholesale banking services. It involves individual and corporate clients, and includes bank transfers, payments and settlements, documentary collections and credits, corporate and household lending, card business and some others (UNCTAD, 2002).[3]

E-Banking is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels.[4]

EVOLUTION OF E-BANKING:

[2] Report on Internet Banking, Reserve Bank of India (DEC.11, 2018)

https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/21595.pdf

[3] The United Nations Conference on Trade and Development, 2002.

[4] N.Krishna Veni (2007), Introduction to E-Commerce, E-Business and E-Banking, Indian MBA.Com (Dec.16, 2018).www.indianmba.com/Faculty Column/ FC545/fc545.html.

Technology in Banking started with the use of punched card machines like accounting machines or ledger posting machines. The use of technology at that time was limited to keeping books of the bank. It further developed with the birth of online real time system and vast improvement in telecommunications during the late 1970's and 1980's and resulted in a revolution in the field of banking to be termed as "Convenience Banking". Through this the bank is carried to the doorstep of the consumer. The 1990's saw the birth of distributed computing technologies and relational data base management system.[5] The Indian economic development took place in the realistic world from 1991 LPG policy. By this, soundest phase for the Indian banking system was adopted by introducing phone banking and net banking for providing satisfactory service to consumers. The entire system focused on satisfactory service to consumers. Time is given more importance than money. The financial system of India has shown a great deal of resilience. All these technological developments took place, since LPG in India ~~has~~ spread a red carpet for the foreign firms which in turn became challenges for the domestic, public sector firms as they were bound to compete with global players.[6]The credit of launching internet banking in India goes to ICICI bank, Citibank and HDFC bank followed by internet banking services in 1999.[7] The Internet Technology started with providing different levels of banking services such as;

(i) The Basic Level Service (Information Only System) where the banks provided disseminated information about their different products and services to the customers and members of public in general. It may receive and reply to customers query through e-mail.

---

[5] The Evolution of Internet Banking Information Technology, Uni Assignment Centre, (Dec.15, 2018). https://www.uniassignment.com/essay-samples/information-technology/the-evolution-of-internet-banking-information-technology-essay.php.

[6] Structure of Banking System and Emergence of E-Banking in India , Shodhganga , (Dec.15, 2018).

http://shodhganga.inflibnet.ac.in/bitstream/10603/28610/10/10_chapter%202.pdf.

[7] Dr.Roshan Lal, Dr. Rajni Saluja, E-Banking: The Indian Scenario, Asia Pacific Journal of Marketing and Management Review, ISSN 2319-2836, Vol.1 (4), December (2012), (Dec.17, 2018).

http://indianresearchjournals.com/pdf/apjmmr/2012/december/2.pdf.

(ii) Simple Transactional Websites (Electronic Information Transfer System) - They do not permit fund based transactions from the account of its customers. But it allows its customers to submit their instructions, applications for different services, queries on their account balances etc.

(iii) Fully Transactional Websites (Fully Electronic Transactional System) - It allows customers to operate on their own accounts for transfer of funds, payment of different bills, subscribing to other products of the bank and to transact purchase and sale of securities etc[8]

The prominent electronic distribution channels are: ATM's, credit cards, debit cards, mobile banking and internet banking.

TRADITIONAL BANKING V. e-BANKING:

Before getting into the context of differentiation, let's first get to know what a traditional banking is? Traditional Banks were the original banks, the financial depository institutions first to offer checkable deposits. They are the checking - account issuing financial intermediaries that must often come to mind when the term 'bank' is used.[9]

Advantages of Traditional Banking over e-Banking:

1. Traditional banks exist physically for serving consumers, while e-banking do not have physical presence as services are rendered online.

[8] Supra Footnote No:3.

[9] Traditional Banks, Encyclonomic WEB* pedia, (Dec.15, 2018).

https://www.AmosWEB.com, AmosWEB LLC, 2000-2018.

2. In traditional banks, customers can have face to face contact with the banking authorities, while in e-banking they have only electronic contacts (i.e.) through e-mail, prescribed website etc.

3. Traditional banking do not encounter e-security threats whereas e-banking is subjected to security threats which is a major problem faced by customers in accessing accounts through internet.[10]

Advantages of E-Banking over Traditional Banking:

1. E-banking does not consume time, as customers do not have to visit banks to check balances in their account, to transfer amount from one account to another account of the same or different bank. They can access their accounts readily from any place and at any time. But, in traditional banking this process is vice-versa i.e. time consumption is high.

2. In case of accessibility, e-banking provides 24 hours access to banking services whereas in traditional banking it can be accessed only during working hours.

3. E-banking facility allows the customers who often travel overseas to have access and control over their finances while by the way of traditional banking they cannot pay close attention in controlling their finances.

[10] Sonia Sharma, A detail comparative study on e- banking VS traditional banking, International Journal of Applied Research 2016; 2(7): 302-307 (Dec.16, 2018).

http://www.allresearchjournal.com/archives/2016/vol2issue7/PartE/2-6-146-742.pdf.

4. The cost of e-banking is much less than traditional banking as e-banking does not require customer to spend money on visiting banks and helps to save on postal charges and operating costs.

5. By taking up the process of online banking, the customers are required not to stand in queues as that of traditional banking.[11]

6. E-banking reduces the burden of branch banking.

Since the e-banking technology has many advantages over traditional banking they are taken up to promote the economic and financial development of a country, as this is an era where time is valued over money. Many big customers have nexus with private and foreign banks having e-banking facility rather than public sector banks. This forced the public sector banks to compete with the advancement of technology, in order to increase their customer base. E-banking is an improvised technology of Traditional banking.

MODELS OF E-BANKING:

For effective implementation of e-banking and to increase the level of technology, certain e-banking models are being suggested. They are;

(i) COMPLETE CENTRALIZED SOLUTION (CCS)[12]: This is a network model, ideal for banking branches in which activities can be implemented uniformly and efficiently. Within this framework, the bank would offer the web server and the software necessary to connect to the master server. The characteristics of CCS are;

[11] Differences between Internet Banking and Traditional Banking, Money Matters (Dec.16, 2018).

https://accountlearning.com/top-10-differences-between-internet-banking-and-traditional-banking/

[12] Growth and Development of Online Banking, Shodhganga, (Dec.17, 2018).

http://shodhganga.inflibnet.ac.in/bitstream/10603/70587/11/11_chapter%203.pdf.

1. The entire system software, data of bank etc are stored in a centralized server with the hot reservoir to be placed in a different place and connected through the high speed and efficient server.

2. The branches nodes are provided online to receive customer requests and provide service across the counter.

3. The nodes under remote twigs are associated all the way through effectual protectorate links with sufficient redundancy for reliability, as well as adequate bandwidth.

4. Skilled labourers are required only in the centralized location.

(ii) FOCUS GROUPS: Under this model, computerized branches are connected to the regional processor located in each of the city which then connects despite trusted medium to a federal high-end server.

For this endeavor, it's necessary that an incorporated mechanization is accessible in all branches, so that the connectivity between different branches can be established through regional cluster.[13]

(iii) RIBERA ALTA TECHNOLOGY: Under this model, high tech shore provide e-banking facilities through certain traditional bank branches and offering customer services in the course of additional branches. Thus technology allows the bank to play a balancing role in providing state of art services to increasingly demanding customers in major cities while continuing to offer personalized services to traditional customers dominating the banking scene.[14]

DEFECTS IN E-BANKING:

E-banking has shown certain defects in its functioning. They are:

[13] Supra Footnote No:13

[14] ibid

1. The agreements formed through electronic media and laws relating to customers disclosure and privacy protection are uncertain.

2. Rights and obligations of the banks and customers are uncertain and the applicability of laws and rules are also ambiguous.[15]

3. The risk of security breach exists. Security is by far one of the major concerns dealing with e-banking, worrying that intruders will get into their account and spend their money. The access of unauthenticated persons in the system is a concern for both clients and banks.[16]

CHALLENGES FACED WITH THE ADOPTION OF E- BANKING:

1. The major threat faced by banking sector is that customers do not consider their e- banking services safe and secure at all times, since they are afraid of the factor that it may cause loss of data or money due to technical defaults.

2. The banks face business challenges also. Since the service charges for transactions through online are very low, they can celebrate profits only when an immense number of transactions are routed over the websites of e-banks.

3. Lack of preparedness is seen on part of both banks and customers in the adoption of incipient technological changes.

[15] Dhananjay B, Suresh Chandra B, Journal of Internet Banking and Commerce, (Nov.29, 2018).

http://www.icommercecentral.com/open-access/the-electronic-banking-revolution-in- india.php?Aid=59261.

[16] Supra Footnote No:11

4. For installation of e-delivery channels, there is a lack of congruous infrastructure.[17]

5. Low awareness among consumers on e-banking.

RISKS ASSOCIATED WITH E-BANKING:

➢ Banks and Customers face various kinds of risks by the way of e-banking. They are;

(i) OPERATIONAL RISK: Also known as transactional risk that takes the form of inaccurate processing of transactions, non enforceability of contracts, problems in data integrity, data privacy and confidentiality, unauthorized access/intrusion to bank's systems and transactions etc. The potential sources of the operational risk are due to inadequacies in technology, negligence on the part of customers and employees, fraudulent activities of bank employees and the act of hackers.

(ii) SECURITY RISK: It arises owing to unauthorized access to bank's critical information stored like accounting system, risk management system, portfolio management system etc. The breach of security may result in loss of data, tampering with customer information, disabling of a significant portion of bank's internal computer system thus denying service by implanting virus etc. This in turn in leads to direct financial loss to the bank.

(iii) RISK BASED ON SYSTEM ARCHITECTURE AND DESIGN: Banks must update their systems based on the prevailing technology. Technology which is outdated, not scalable or not proven could result in investment loss to the bank.

(iv) REPUTATIONAL RISK: This arises due to the banks own action or third party action which leads to negative public opinion. This risk

[17] Reeta Clonia, M.Asht, E-banking in India: Current and future prospects, Research Gate (Dec.17, 2018).

https://www.researchgate.net/publication/308222670_E-banking_in_India_Current_and_future_prospects.

may also arise when the system or product is not working to the expectations of the customers. Losses occur when customers view other banks offering the same type of services with suspicion.

(v) MONEY LAUNDERING RISK that arises due to inappropriate rules.

(vi) CREDIT RISK arises when the customer will not settle an obligation for full value either when due or at anytime thereafter.[18]

RISK MANAGEMENT:

Risk management is carried out by following the standards as laid down in the guidelines put forth by the Reserve Bank of India (RBI) and according to the provisions as laid down in Information Technology Act, 2000.

The banks before offering Internet banking with transactional facility have to get prior approval of the RBI, but this is not mandatory in case of banks offering Internet banking (view only) facility. After getting approval in order to extend the service the bank have to submit a report containing the business plan, cost and benefit analysis, operational arrangements like technology adopted, business partners, third party service providers systems and control procedures that the bank proposes to adopt for managing risks, to the regional officer of the RBI.

(i) Technology and Security Standards:

- ➢ Logical access controls to data, systems, application software, utilities, telecommunication lines, libraries, system software, etc should be in place.

- ➢ All computer accesses including messages received should be logged.

[18] Reeta Clonia, M.Asht, E-banking in India: Current and future prospects, Research Gate (Dec.17, 2018).

https://www.researchgate.net/publication/308222670_E-banking_in_India_Current_and_future_prospects.

- ➢ Security violations should be recorded and follow up action must be taken.

- ➢ Banks should acquire necessary tools to avoid security breaches and must duly review their security infrastructure and security policies and optimize them in the light of their own experiences and changing technologies.

- ➢ The Information Security Officer and the Information System Auditor should conduct periodic penetration tests by attempting to guess passwords using password cracking tools, by engaging outside experts like hackers etc.

- ➢ The banks should have proper infrastructure and schedules for backing up data to ensure recovery without loss of transactions.

- ➢ Banks should periodically update the systems to newer versions which give better security and control.[19]

(ii) Legal Standards:

- ➢ Banks may provide Internet Banking facility to a customer only at his/her option based on specific written or authenticated electronic requisition along with a positive acknowledgement and after verification of the identity of the customer and adherence to KYC guidelines.

[19] Internet Banking Facility for Customers of Cooperative Banks, Notifications, Reserve Bank of India (Dec.11, 2018). https://rbi.org.in/Scripts/NotificationUser.aspx.

- The provisions of the Information Technology Act, 2000, and other legal requirements need to be scrupulously adhered to while offering internet banking.

- The Consumer Protection Act, 1986, defines the rights of consumers in India and is applicable to banking services as well. The rights and liabilities of customers availing of internet banking services need to be clearly explained to customers opting for internet banking. Considering the banking practice and rights enjoyed by customers in traditional banking, the bank's liability to the customers on account of unauthorized transfer through hacking, denial of service on account of technological failure etc needs to be assessed and banks providing internet banking should insure themselves against such risks.[20]

LEGAL BACKGROUND:

In India, banks can avail the e-banking facility only after getting prior approval from the RBI. Banks with internet banking (view only) facility or transactional facility are bound by the rules, regulations and guidelines as laid by the Reserve Bank of India.

The Information Technology (IT) Act, 2000 was amended in 2008 to include certain provisions relating to the offences associated with the electronic banking and the punishments imposed thereof for a stronger data protection and to combat cyber crimes. Section 43-85 of the IT Act, 2008 deals with offences and punishments with regards crimes against e-banking. Chapter IX & XI - deals with penalty, compensation, adjudication and offences.

- **Section.43**- Imposes a maximum penalty of one crore rupees when there is any damage to computer, computer system or computer

[20] ibid.

network or for accessing or extracting any data. If this, when done by a person fraudulently or dishonestly then according to **section.66,** he/she will be punishable with maximum of 2-3 years imprisonment or with fine which may extend to five lakh rupees or both.

- **Section.43A**- Imposes a maximum of five crore rupees as compensation for failure to protect sensitive data by body corporate.

- **Section.65**- Tampering with computer source documents - punishable with imprisonment upto 3 years or fine which may extend to two lakh rupees or with both.

- **Section.66B**- Punishment for dishonestly receiving stolen computer resource or communication device is punishable with an imprisonment which may extend to 3 years or fine which may extend to one lakh or with both.

- **Section.66C**- Punishment for identity theft. Fraudulently or dishonestly making use of the electronic signature, passwords or any other unique identification are punishable with an imprisonment which may extend to 3 years or with fine which may extend to one lakh rupees.

- **Section.66D**- Punishment for cheating by personation by using computer resource is imprisonment which may extend to 3 years or with fine which may extend to one lakh rupees.

- **Section.66E**- Punishment for violation of privacy is 3 years imprisonment and fine not exceeding two lakh or with both.

- **Section.66F**- Cyber Terrorism is punishable with an imprisonment which may extend to imprisonment for life.[21]

Apart from the security granted by these provisions, banks should also carry out encryption process for protection of consumers' data and privacy.

CONTRIBUTION BY e-BANKING TO DIGITIZATION OF INDIA:

The agenda for Digital India is to ensure that the government services are availed by the public electronically by improving the online sources and by increasing the internet connectivity in order to digitally empower the field of technology. This was launched on 2 July, 2015 with an initiative to connect all rural areas with high speed internet connectivity. Digital India consists of three core components, they are: the creation of digital infrastructure, delivering services digitally and digital literacy.

Digital Transformation in banking, that is from traditional banking to e-banking sprouted with the varying needs of consumers such as: reward me for my business, simplify my life by providing "any time, any place access to my account", know me as a person, look out for me by providing me with wealth building advice and anticipate my needs by telling me what I am spending and how I can save. This led to the change in banking process from single channel to bi-directional channel.

India's first digital village is Akodara in Sabarkantha district of Gujarat. The village with a total population of 1191 people and 250 household used a cashless system for payment of goods and services. All transactions in the village are carried out through digital modes like SMS, net banking or debit cards. By digital village project in 2015 this village was adopted by ICICI bank and all important transactions like

[21] The Information Technology Act, 2008 as amended by Information Technology Amendment Bill 2006 passed in Lok Sabha on Dec. 22nd and in Rajya Sabha on Dec. 23rd of 2008.

selling of agricultural produces, milks at local markets and societies were made cashless.[22]

Demonetization in 2016: The main intention behind demonetization was to control black money and to increase e-transaction in the country. Hence, after demonetization in 2016, e-banking has became an important aspect for economic advancement and development. Many online wallets were made available such as Generic Online, e-Wallet, Paytm etc. Now the government is planning to bring a e-Wallet of its version as a move towards cashless society and to create a change in the trend of purchases and transfers. Demonetization has led to wave of e-banking in India and the society is moving towards cashless and paperless transactions.[23]

CONCLUSION:

e-Banking was initialized with the advancement of the technology in order to ensure economic and financial development in the country. e-banking facility though very useful was not utilized by many consumers due to lack of awareness. Awareness regarding e-banking must be created among public through various classes, programs etc. The rights and liabilities of consumers as well as banks, information regarding the procedures to be followed, the way to tackle a technical default when occurs, have explained to be clearly to the consumers. Security over consumers' information and data privacy have to be ensured abiding by the rules and provisions laid down and by incorporating the appropriate technology.

REFERENCES:

[22] Chandrawati Nirala, Dr. BB Pandey, Role of E-Banking services towards Digital India, International Journal of Commerce and Management Research ISSN: 2455-1627(Dec.18, 2018).

www.managejournal.com/download/421/3-3-14-233.pdf.

[23] D.Mounika, R.Kadhirvel , Impact Of Demonetization In E-Banking, International Journal of Scientific & Engineering Research, Volume 8, Issue 4, April-2017, ISSN 2229-5518 (Dec.18, 2018).

https://www.ijser.org/researchpaper/Impact-Of-Demonetization-In-E-Banking.pdf.

- Shilpan Dinesh Kumar Vyas, Impact of E-Banking on Traditional Banking Services, Research Gate (Dec.16, 2018). https://www.researchgate.net/publication/258726999-Impact-of-E-Banking-on-Traditional-Banking-Services.

- Report on Internet Banking, Reserve Bank of India (DEC.11, 2018) https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/21595.pdf

- N.Krishna Veni (2007), Introduction to E-Commerce, E-Business and E-Banking, Indian MBA.Com (Dec.16, 2018). www.indianmba.com/Faculty Column/FC545/fc545.html.

- The Evolution of Internet Banking Information Technology, Uni Assignment Centre, (Dec.15, 2018). https://www.uniassignment.com/essay-samples/ information-technology/the-evolution-of-internet-banking-information-technology-essay.php.

- Dr.Roshan Lal, Dr. Rajni Saluja, E-Banking: The Indian Scenario, Asia Pacific Journal of Marketing and Management Review, ISSN 2319-2836, Vol.1 (4), December (2012), (Dec.17, 2018). http://indianresearchjournals.com/pdf/apjmmr/2012/december/2.pdf.

- Structure of Banking System and Emergence of E-Banking in India, Shodhganga, (Dec.15, 2018). http://shodhganga.inflibnet.ac.in/bitstream/10603/28610/10/10_chapter%202.pdf.

- Traditional Banks, Encyclonomic WEB* pedia, (Dec.15, 2018).

https://www.AmosWEB.com, AmosWEB LLC, 2000-2018.

- Sonia Sharma, A detail comparative study on e- banking VS traditional banking, International Journal of Applied Research 2016; 2(7): 302-307 (Dec.16, 2018). http://www.allresearchjournal.com/archives/2016/vol2issue7/PartE/2-6-146-742.pdf.

- Differences between Internet Banking and Traditional Banking, Money Matters (Dec.16, 2018). https://accountlearning.com/top-10-differences-between-internet-banking-and-traditional-banking/

- Growth and Development of Online Banking, Shodhganga, (Dec.17, 2018). http://shodhganga.inflibnet.ac.in/bitstream/10603/70587/11/11_chapter%203.pdf.

- Dhananjay B, Suresh Chandra B, Journal of Internet Banking and Commerce, (Nov.29, 2018). http://www.icommercecentral.com/open-access/the-electronic-banking-revolution-in-india.php?aid=59261.

- Reeta Clonia, M.Asht, E-banking in India: Current and future prospects, Research Gate (Dec.17, 2018). https://www.researchgate.net/publication/308222670_E-banking_in_India_Current_and_future_prospects

- Internet Banking Facility for Customers of Cooperative Banks, Notifications, Reserve Bank of India (Dec.11, 2018). https://rbi.org.in/Scripts/NotificationUser.aspx.

- D.Mounika, R.Kadhirvel , Impact Of Demonetization In E-Banking, International Journal of Scientific & Engineering Research, Volume 8, Issue 4, April-2017, ISSN 2229-5518 (Dec.18, 2018).
  https://www.ijser.org/researchpaper/Impact-Of-Demonetization-In-E-Banking.pdf.

- Chandrawati Nirala, Dr. BB Pandey, Role of E-Banking services towards Digital India, International Journal of Commerce and Management Research ISSN: 2455-1627(Dec.18, 2018).
  www.managejournal.com/download/421/3-3-14-233.pdf.

- E-Banking in India and its present scenario and future prospects, Basavaraj MT, Academia.
  http://www.academia.edu/5337192/_E-BANKING_IN_INDIA_AND_ITS_PRESENT_SCENARIO_AND_FUTURE_PROSPECTS_

- R. K. Uppal, Rimpi Jatana, E-Banking in India Challenges & Opportunities (Western Books Corporation)

- Manikyam Ratna K. Indian Banking Sector-Challenges and Opportunities, IOSR Journal of Business and Management. 2014; 16(2):52-61

STATUTES:

- The Information Technology (Amendment) Act, 2008.

- The Reserve Bank of India Act, 1934.

- The Consumer Protection Act, 1986.

THE INTRICACIES AND IMPLICATIONS OF ELECTRONIC FUND TRANSFER IN INDIAN BANKING

P. SIVATHAS*

ABSTRACT:

There has been an extensive expansion of the financial system of India, in which Banking sector played an important role. After the Back Office Automation phase and Front Office Automation phase in banking technology, the third phase of connecting customers electronically to their Accounts was started in mid 1980s. The fourth phase began with system integration and connecting customers to all banking operations electronically. Electronic banking has emerged from such an innovative development. There are more plastic cards in our wallet than currency notes. Debit cards remain the most preferred way of carrying out transactions as compared to credit cards. E-Banking comprises mainly electronic funds transfer and usage of online banking services. Electronic banking was offered by the international banks initially, since flow of digital cash was not predominant in the Indian market until the advent of demonetization. After demonetization in November 8, 2016, the mode of fund transfer gradually increased through electronic means. Based on RBI guidelines, six Indian public sector banks, two private banks and 2 international banks jointly invested and created non profitable NPCI (National Payment Corporation of India), which regulates internal transactions and electronic fund transactions in India. Thereby UPI (Unified Payment Interface) and BHIM Mobile Application (Bharat Interface for Money) were launched. However, it has its own limitations and challenges when we talk about security. The present study is an attempt to examine and analyze the challenges that are being faced in Electronic Fund Transfer in Indian banking, opportunity to increase awareness and measures adopted for safe and secure Electronic Fund Transfer.

* Ph.D. Scholar, The Tamilnadu Dr. Ambedkar Law University, Chennai and Assistant Professor, Government Law College, Dharmapuri.

Research Methodology:

This research paper has been studied on the basis of RBI's circulars to banks and secondary data referred from various research articles and certified journal publications.

1. Introduction

The payment and funds transfer sources were limited to physical methods such as direct currency exchange or a written cheque method. With the emergence of internet and mobile banking and the emerging e-commerce opportunities, banks have marched ahead with introducing the concept of electronic funds transfer, which stepped much more after demonetization in the year 2016 in India. Today, electronic funds transfer allows you to exchange funds between individuals, as well as organizations via electronic gateways which can be accessed using internet, computers, mobile phones, tabs and smart phones. Funds can be transferred instantly from one account to another, either within the same bank or to a different bank network or to a Virtual Payment Address (VPA) at any given time.

2. Electronic Fund Transfer (EFT)

2.1 Meaning of EFT and Electronic money

The word 'electronic' means a device having or using many small parts, such as microchips, that control and direct a small electric current[1]. The Word 'fund' means an amount of money that has been saved or has been made available for a particular purpose[2]. The word 'transfer' means something or somebody moves from one place to another[3]. EFT means the transfer of money from one bank account to another, either within a single financial institution or across multiple institutions, via computer based system, without the direct intervention of bank staff[4]. In order to execute an EFT, the involvement of three banks i.e. sending bank, participating bank and beneficiary bank and the customer's initiation is must. Various guidelines are prescribed by the RBI to all the above said banks to maintain the security, integrity

[1] Oxford Advanced Learner's Dictionary – Oxford University Press.
[2] Oxford Advanced Learner's Dictionary – Oxford University Press.
[3] Oxford Advanced Learner's Dictionary – Oxford University Press.
[4] https://en.wikipedia.org/wiki/Electronicfundtransfer accessed on December 10, 2018.

and efficiency of the system[5]. Electronic money is a store of monetary value, held in digital form, which is available for immediate exchange in transaction[6]. It is an electronic replacement of for physical cash. It has no intrinsic value, 'numbers are money here'. Electronic money is possible through cryptography and digital signature. Private keys are used to sign (identification) and public key is used to encrypt (security).

2.2 Facility and types in transformation of funds electronically

Transferring funds via electronic gateway is much simpler than the conventional methods. One can choose to:-

a) Transfer funds into one's own linked accounts of the same bank network.
b) Transfer funds into a different account of the same bank.
c) Transfer funds into different bank's accounts using NEFT, RTGS IMPS and BHIM UPI.
d) Transfer through ECS and NACH.
e) Transfer through POS by debit cards, credit cards and Prepaid Payment Instruments.

2.2.1 NEFT

The National Electronic Funds Transfer (NEFT) is an electronic fund transfer system maintained by the Reserve Bank of India (RBI). This system was started in November 2005 and the setup was established and maintained by IDRBT[7]. NEFT is a nation-wide money transfer system which allows customers with the facility to electronically transfer funds from their respective bank accounts to any other account of the same bank or of any other bank network. Not just individuals but also firms and corporate organizations may use the NEFT system to transfer funds to and fro. Funds transfer through NEFT requires a transferring bank and a destination bank. Before transferring funds via NEFT one has to register the beneficiary account detail who is receiving funds. Any sum of money can be transferred using the NEFT system with a maximum of Rs.10,00,000/-. NEFT transactions can be

[5] https://www.rbi.org.in/scripts/bs-viewcontent accessed on December 10, 2018.
[6] School of Library and Information Science.
http://info.ils.indiana.edu/~hrosenba/L561/classes/emoney/emoney.ppt.
[7] Institute for Development and Research in Banking Technology,
https://en.wikipedia.org/wiki/National.Electronic-fund-transfer accessed on December 10, 2018.

ordered anytime, even on holidays except for Sundays which are designated bank holidays but ***processed and settled during the specified NEFT hours in batches*** defined by the Reserve Bank of India depending upon specific time slots. Recently, there were 24 settlement batches operating at present between the time slot of 8 am to 7 pm on weekdays and from 8 am to 1pm on Saturdays with 12 settlement batches. At the end of March 2018, the NEFT facility was available through 1,40,339 branches of 192 banks, in addition to a large number of business correspondent (BC) outlets[8].

2.2.2 RTGS

Real Time Gross Settlement (RTGS), as the name suggests is a real time funds transfer system which facilitates one to transfer funds from one bank to another in real time or on a gross individual basis. The transaction is not put on a waiting list and cleared out instantly. RTGS payment gateway, maintained by the Reserve Bank of India makes transactions between banks electronically. The transferred amount is instantly deducted from the account of one bank and credited to the other bank's account. Users such as individuals, companies or firms can transfer large sums using the RTGS system. The minimum value that can be transferred using RTGS is Rs.2 Lakhs and above. However there is no upper cap on the amount that can be transacted.

2.2.3 IMPS and MMID

Majority of the funds transferred using electronic channels are processed via NEFT or RTGS. But as the funds could only be cleared in batches using these transfer gateways, the National Payments Corporation of India (NPCI) introduced a pilot mobile payment project also known as the Immediate Payment Service (IMPS). IMPS service was publicly launched on November 22, 2010[9].

The IMPS service features a secure transfer gateway and an immediate confirmation on fulfilled orders. IMPS are offered on all the cellular devices via Mobile Banking or through SMS facility. To be able to transfer money via IMPS route one must first register for the immediate payment services with bank. On obtaining the Mobile Money Identifier (MMID) and MPIN from the bank one can make a request via SMS to transfer a certain amount to a beneficiary. To initiate an IMPS transfer one must enter the beneficiary's mobile number,

[8] https://www.rbi.org.in/scripts/AnnualReportPublications.aspx?Id=1236 accessed on December 13, 2018.
[9] National Payments Corporation of India". www.npci.org.in. Retrieved 2017-07-26.

beneficiary MMID, the transfer amount and transferor's secret MPIN while requesting the fund transfer. As soon as the transaction is cleared, transferor will receive a confirmation SMS and the transaction reference number. In the meanwhile, the money is credited into the beneficiary's account.

Now-a-days, two type of IMPS transfer facility is allowed; one through mobile phone using MMID and another through bank mobile application using smart phone to make IMPS fund transfer to one's account number directly using bank account details or through MMID. The cap on the maximum value through IMPS transfer is Rs.1 Lakh, whereas for quick instant transfer without adding a beneficiary is Rs.10 Thousand only.

2.2.4 BHIM UPI and Mobile banking Apps

Based on RBI guidelines, 6 Indian public sector banks, 2 private banks and 2 international banks jointly invested and created non-profitable NPCI in the year 2008. It regulates electronic fund transactions and integrates the small retail transactions between banks in India through UPI (Unified Payment Interface) and BHIM Mobile Application (Bharat Interface for Money)[10]. UPI is an electronic funds transfer instrument that enables all bank account holders to send and receive money from their smart phones without the need to enter bank account information or net banking user id/password. This requires only the recipient's mobile number or Virtual Payment Address (VPA).

Now-a-days many mobile phone applications (mobile wallets) are coming into the market through service providers, to do banking transactions electronically for bill payment, recharge of prepaid mobile and e-commerce activities. The android applications can be classified into bank applications and Virtual e-wallet or Virtual Money bank. Some of the applications are

a) Axis Bank Lime and Axis Mobile
b) HDFC bank mobile banking App and PayZapp
c) ICICI Pockets, iMobile
d) SBI Buddy, State Bank Anywhere Personal and YONO
e) SIB Mirror
f) BHIM UPI App
g) Kotak-811 & Mobile banking App
h) Canara Bank Mobile banking App
i) IPPB mobile bank App (Virtual Bank)
j) Jio Money
k) Mobikwik

[10] Dinamani Newspaper, Dharmapuri Edition, page 6, dated November 19, 2018.

l) mRupee
m) Paytm
n) Airtel Money
o) Vodafone M-pesa
p) IndPay
q) IRCTC
r) OlaMoney
s) PayU
t) Razarpay
u) PhonePe etc.,

2.2.5 ECS, NACH and APB

ECS is an electronic mode of funds transfer from one bank account to another. It can be used by institutions for making payments such as distribution of dividend interest, salary, and pension, among others. It can also be used to pay bills and other charges such as telephone, electricity, water or for making equated monthly installments, payment on loans as well as SIP investments. ECS can be used for both credit and debit purposes[11]. Customers need to inform the bank and to provide a mandate. It authorizes the institution (payee or beneficiary), who can then debit or credit the payments through the bank. The mandate contains details of Customer's bank branch and account particulars. Customer will know the money has been debited from his account through mobile alerts or messages from the bank. The ECS user can set the maximum amount beneficiary customer can debit from the account, specify the purpose of debit, as well as set a validity period for every mandate given.

National Automated Clearing House (NACH) is a centralized system, launched with an aim to consolidate multiple ECS systems running across the country and provides a framework for the harmonization of standard & practices and removes local barriers/inhibitors. The NACH system provides a robust, secure and scalable platform to the participants with both transaction and file based transaction processing capabilities. NACH's Aadhaar Payment Bridge (APB) System, developed by NPCI has been helping the

[11] http://www.business-standard.com/article/pf/what-is-electronic-clearing-service-ecs-111070800019_1.html accessed on March 18, 2018.

Government and Government Agencies in making the Direct Benefit Transfer scheme a success.

2.2.6 POS terminal, debit and credit cards and Prepaid Payment Instruments

Now, there are more plastic cards in our wallet than currency notes. Debit cards remain the most preferred way of carrying out transactions as compared to credit cards. Prepaid payment instruments are methods that facilitate purchase of goods and services against the value stored on such instruments, the value being paid for by the holder, by cash, by debit to a bank account, or by credit card. The prepaid instruments can be issued as smart cards, magnetic stripe cards, internet accounts, online wallets, mobile accounts, mobile wallets, paper vouchers and any such instruments used to access the prepaid amount.

3. Characteristics of interbank Electronic Fund Transfer (EFT)

The most important characteristics of the interbank electronic funds transfer are:

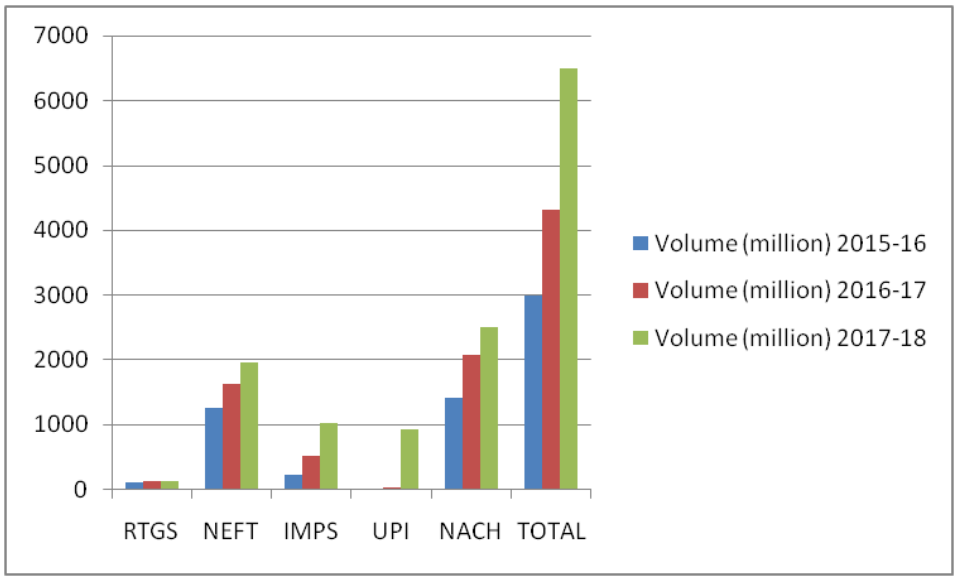
a) The transfer is made after a transfer order addressed to a bank which is a central bank (participating bank), where the two bank accounts (sending bank and receiving bank) and the funds transferred is the central bank money.
b) The transfer could be made in real time (from some seconds to some minutes) or could be made in a bank day.
c) The transfer could be individual (gross settlement processed separately) or net transfer: suppose the calculus of the reciprocal net financial position between every two banks, which represents the result of the all reciprocal sending's and receiving's of funds by a day and generally until a fixed and known date.
d) The transfer could be; Domestic (national) – the orders transfer are addressed to the central bank; or Transfrontalier (international) – the orders transfer are addressed to the bank agreed by all banks in the system.
e) The systems could be used by the participants to make different types of payments; between persons - P2P[12], between persons and companies -

[12] Person to Person

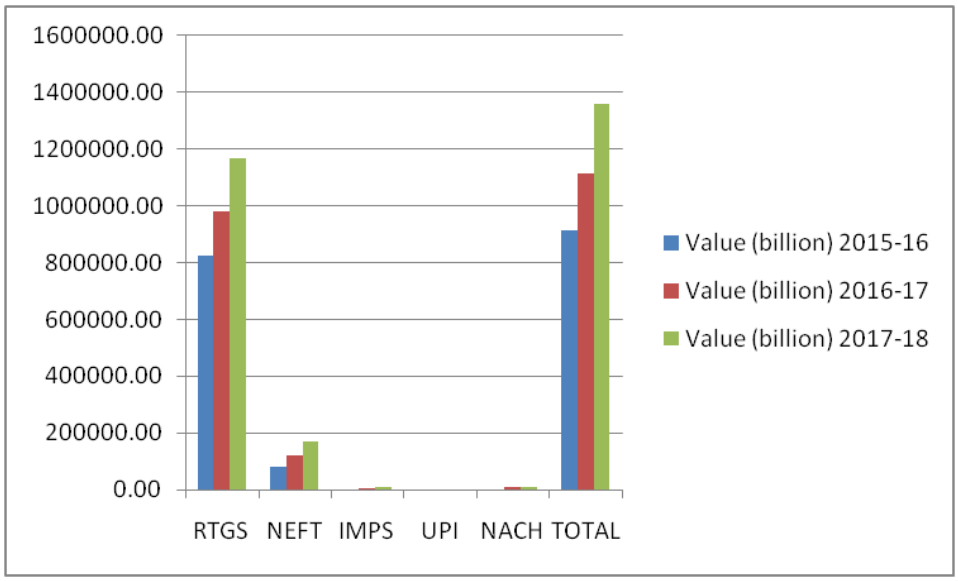
B2C[13], between companies - B2B[14], to the central or local administration (P2G[15] & B2G[16]).

4. Growth in Electronic Fund Transfer

Between the electronic funds transfer, the interbank electronic transfer has the big volume of money transfer, both number of transaction and the value of the transferred funds. After demonetization in November 8, 2016, the mode of fund transfer gradually increased through electronic means.



[13] Business to Customer
[14] Business to Business
[15] Person to Government
[16] Business to Government



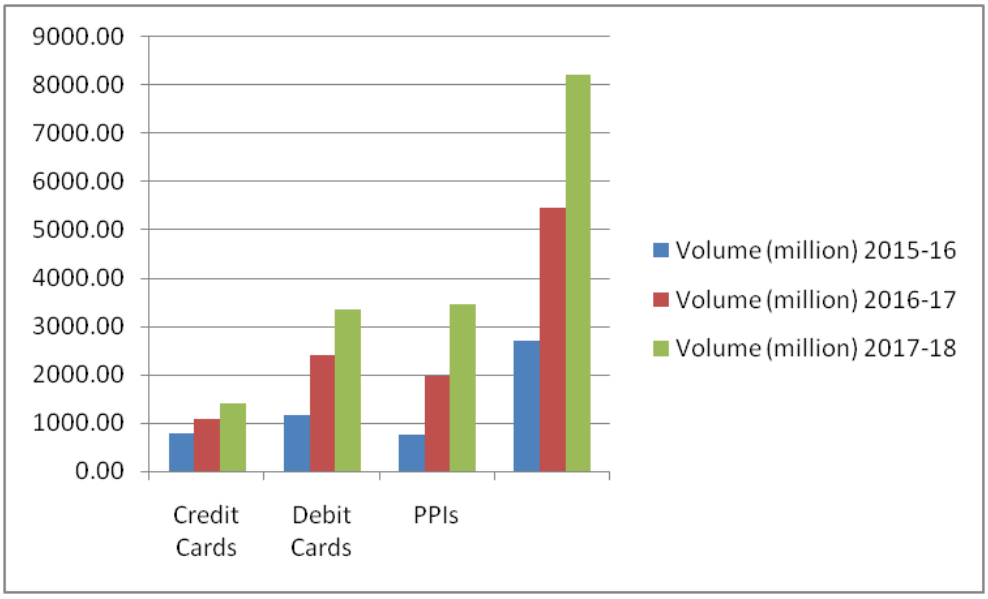
The payment and settlement systems recorded robust growth in 2017-18, with volume and value growing at 44.6 per cent and 11.9 per cent, respectively, on top of an increase of 56.0 per cent and 24.8 per cent, respectively in 2016-17. The share of electronic transactions in the total volume of retail payments increased to 92.6 per cent in 2017-18, up from 88.9 per cent in the previous year with a corresponding reduction in the share of paper based clearing instruments from 11.1 per cent in 2016-17 to 7.4 per cent in 2017-18[17].

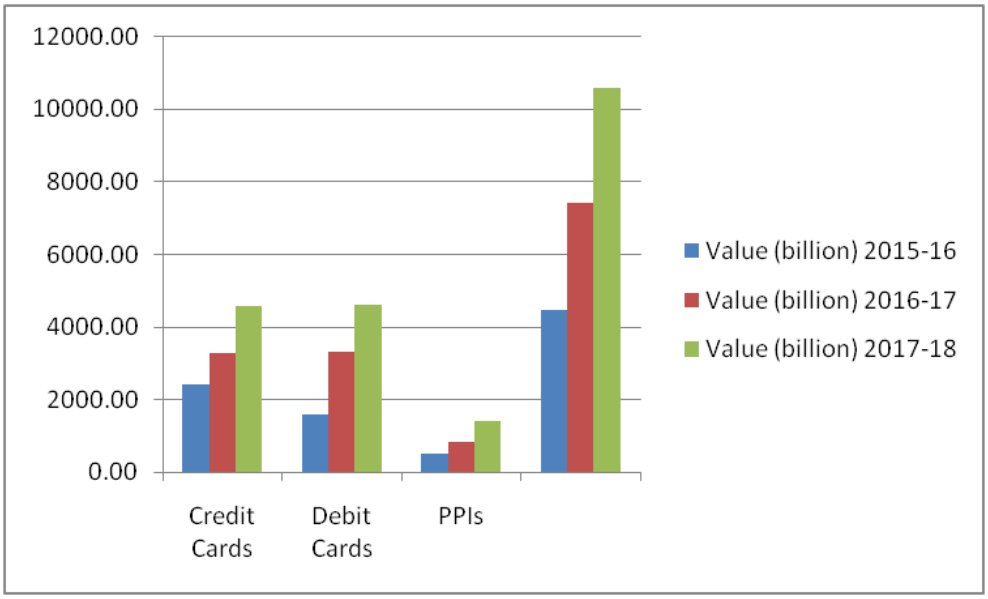
Amongst the electronic modes of payments, the RTGS system handled 124 million transactions valued at Rs.1,167 trillion, in 2017-18, up from 108 million transactions valued at Rs.982 trillion, in the previous financial year. At the end of March 2018, the RTGS facility was available through 1,37,924 branches of 194 banks. The NEFT system handled 1.9 billion transactions valued at around Rs.172 trillion, in 2017-18, up from 1.6 billion transactions valued at Rs.120 trillion, in the previous financial year, registering a growth of 20 per cent in terms of volume and 43.5 per cent in terms of value.

During 2017-18, the number of transactions carried out through credit cards and debit cards was 1.4 billion and 3.3 billion, respectively. Prepaid payment instruments (PPIs) recorded a volume of about 3.5 billion transactions, valued at Rs.1,416 billion. Mobile banking services witnessed a growth of 92 per cent and 13 per cent in volume and value terms, respectively,

[17] https://www.rbi.org.in/scripts/AnnualReportPublications.aspx?Id=1236 accessed on December 13, 2018.

while the number of registered customers rose by 54 per cent to 251 million at end-March 2018 from 163 million at end-March 2017[18].





5. Advantages in EFT

It is clear, electronic payment systems have a range of pros in comparison to traditional banking services[19]. They are:

[18] https://www.rbi.org.in/scripts/AnnualReportPublications.aspx?Id=1236 accessed on December 13, 2018.

a) Time savings

Money transfer between virtual accounts usually takes a few minutes, while a paper transfer or wire transfer or a postal one may take several days. Also, there is no need to waste our time waiting in lines at a bank or post office.

b) Expenses control

In EFT, it is easy to maintain data, and thereby by verifying the transactions happened one can bring his disbursements under control, whereas it is necessary to be patient enough to write down all the petty expenses in traditional methods.

c) Reduced risk of loss and theft

Since there is no physical money kept in our wallet or somewhere, it cannot be taken away by robbers.

d) Low commissions or charges

Compare to traditional banking fund transfer, in electronic payment system fee or charges is less than 1% of the total amount and this is a considerable advantage.

e) User-friendly

Usually every service is designed to reach the widest possible audience, so it is easily understandable user interface. In addition, there is always the opportunity to submit a question to a support team or customer care team which often works 24/7.

f) Convenience

All the transfers can be performed at anytime, anywhere with the help of Internet.

6. Disadvantages in EFT

Every new technology has its own minus, even though the invention is introduced for human community development. Some minus in the electronic fund transfer technology are:

a) Restrictions

Each payment system has its limits regarding the minimum and maximum amount in the account, the number of transactions per day and the amount of output.

[19] https://unichange.me/articles/advantages_of_electronic_payment_systems accessed on December 8, 2018.

b) The risk of being hacked

The worse situation is when the system of processing data has been broken, because it leads to the leak of personal data of cards and its owners. Even if the electronic payment system does not launch plastic cards, it can be involved in scandals regarding the Identity theft.

c) The problem of transferring money between different payment systems

Usually the majority of electronic payment systems do not cooperate with each other. In this case, one has to use the services of e-currency exchange, and it can be time-consuming.

d) The lack of anonymity

The information about all the transactions, including the amount, time and recipient are stored in the database of the payment system. And it means the intelligence agency has an access to this information.

e) The necessity of Internet access

If Internet connection fails, one cannot get to online account.

7. Measures to face EFT challenges

a) Ethical hacking

To combat cyber insecurity, many banks and companies including ecommerce and mobile app based service providers are increasingly roping in ethical hackers to look for loopholes in their system by continuously trying to hack into them from outside and report back to the company. Sometimes these ethical hackers also help companies fix the glitch[20].

b) Choosing e-Banking Configuration

E-banking systems rely on a number of common components or processes like Website design and hosting, Firewall configuration and management, Intrusion detection system or IDS (network and host-based), Network administration, Security management, Internet banking server, Internal network servers, Core processing system, Programming support and Automated decision support systems.

[20] Gayathri Nayak, 'With internet banking on the rise, frauds are just a click away', Mumbai Ed., The Economic Times, 5th June, 2003, p.6.

These components work together to deliver e-banking services. Each component represents a control point to consider. Through a combination of internal and outsourced solutions, management has many alternatives when determining the overall system configuration for the various components of an e-banking system.

c) Reporting of frauds

In order to reduce, rather eliminate incidences of frauds and cyber frauds in the country, frauds should be immediately reported to Reserve Bank, in consonance with its classification and guidelines[21].

d) Eliminating multiple authentication by the use of biometric technology

Innovations like Biometric technology allows the person to be identified uniquely by evaluating one or more distinguishing biological traits like face, hand, retina, voice and ear features. The use of biometric authentication can eliminate the requirement of multiple passwords and PIN codes. The Indian banking sector is also gradually adopting biometric authentication to provide simple and secure banking experience to its customers[22].

8. Precautionary measures in using EFT

a) at ATM Booth

Checking for the fixation of skimmer tool at ATM Booth around card Reader Slot area, avoiding to take help of outsiders at ATM Booth, securing ATM card and its PIN and linking one's mobile phone number with bank account are some precautionary measures.

b) on online transactions:

Always login through genuine homepage or secured page by checking the correct URL (Website domain name starts with "https") and check for Key loggers, accessing the online banking account at Cyber cafes. While transacting, disable location services when using

[21] Article by Varun Tripathi on "Frauds and Cyber Frauds in Banking Sector", SCC Online Web edition, accessed on Dec 27, 2017.

[22] Dun & Bradstreet, "Emerging Technologies in digital banking in India", Forbes India, published on August 23, 2017 accessed on February 24, 2018.

apps and protect the computer by installing antivirus software or Anti-malware. Remember to log off when work done and never access the online bank account or banking application in free Wi-Fi Zone. It is safe to keep mobile phones or tabs or laptops or PC applications secure through strong password/screen lock/pattern lock/PIN lock, log out of those sites once transactions are completed and turn off Wi-Fi, Data connection and Bluetooth, when not in use.

c) using mobile app for banking transactions

When we are new to payments via mobile apps, then one can mostly look at going either with mobile wallets or apps supporting UPI payments, depending upon the requirement.

Conclusion

In India, we have no dedicated Internet banking laws but the Reserve Bank of India (RBI) has issued some guidelines in this regard.
However, Internet banking risks in India are high and even RBI acknowledged risks of e-banking in India. Electronic fund Transfer technology has presented the opportunity to create new methods to ease financial burden, start from the individual, state, country and world level. IMPS stands out as the most convenient and instant mode of money transfer, allowing transfer of money across various accounts and banks on the go using a mobile device. This study shows the increasing value and volume of electronic fund transfer systems with many advantages and understands that various short comings such as internet facility, technology cost and some difficulty in dealing with the technology of money transfer also exists.

Many people used electronic fund transfer systems because of the benefits associated with them. Among the most preferred benefits is efficiency, while others that come in where reliability and speed. Most of the people are willing to bear any cost of an EFT as it is efficient. However, shortcomings associated with EFT are found to have a significant effect, therefore attention needs to be focused on the awareness, precautionary measures and secure Electronic Fund Services.

References

1. Andam, Z.R.B. (2003), “e-commerce and e-business” Available at: www.apdip.net/publications/iespprimers/eprimer_eCom.pdf accessed on January18, 2007.

2. Katherine L. Cason (1998), Electronic Benefits Transfer: New Strategies for Improving Public Assistance Programs 6, December 7, 1998.
3. Kepha Nyankora Getembe *etd (2013),* Electronic money transfer systems and business process management among commercial Banks in Kenya, European Scientific Journal April 2013 edition vol.9, No.10 ISSN: 1857–7881 (Print) e -ISSN 1857-7431.
4. Laudon, C. Kenneth and Traver, Carol (2010), E-Commerce, New Delhi: Pearson Education.
5. Codruta poenar (2008), A Study Looking the Electronic Funds Transfer Revista Informatics Economic nr.3(47)/2008.
6. Sander, K.K.C, and Mukwana P, (2003), Money Transfer Systems: The Practice and Potential for Products in Kenya.
7. Volume and Value charts, www.rbi.org.in/accessed on December 10, 2018.

'E-WALLET INDIA- THE ENVISAGED MIRAGE'

S. DHEERA KANISHKA*

ABSTRACT

While cashless transactions are a comfort and the future of this world, the concept is being pushed without tending to two basic concerns - privacy and protection of computerized exchanges. On account of e-wallets, laws setting up security prerequisites and liabilities are absent. With the rapid development of information technology in India, digitalization has been an adopted son for everyone. After the demonetisation scheme of the Indian government privacy and security are the emerging issues in e-commerce. The paper discusses the standard form of contracts, data privacy/protection issues in e-commerce and the draft Data Protection Bill, 2018 submitted by the Justice BN Srikrishna committee. Currently, privacy is considered as a public issue, a proper mechanism is needed for the enforcement of data privacy in e-commerce. The paper also throws light on various landmark judgments of privacy concern in data privacy.

INTRODUCTION

An electronic wallet can be characterized as a virtual cashless administration which can supplant hard money notes. For buying anything, the individual need not rush to ATMs or to the banks to pull back money, rather exchange can be done there and after that in fraction of seconds. It has turned into an upcoming method for buying products and enterprises without any need for hard cash. The fundamental goal of e-wallets is to make speedy exchanges without depending on hard cash or traditional way of transactions. This blast is the eventual outcome of Demonetization in India.

There are numerous applications like Paytm, freecharge, mobikwik etc. which can be downloaded and used for different purposes like making bill payments, doing online shopping, recharging phones etc. Some of these applications have their own portals and a person can perform all the above mentioned and many more tasks via app itself. In all these applications, a person has to link his credit/debit card number with the application to make use of services provided by app. This paper also discusses different characteristics, various needs and risks of electronic payments. The author

* 4th year, Semester – VIII, D.S. National Law University, Visakhapatnam.

agrees on the fact that e-wallets allow the users to enjoy comfortable and easy going platform to shop and pay, that too in minimal possible time.[1]

STANDARD FORM OF CONTRACTS BETWEEN E-WALLET COMPANIES AND ITS USERS

Principles of a valid contract are agreement, which consists of offer and acceptance, intention to create legal relations and the consideration. The nature of contracts between e-wallet companies and its users are of a standard form. Online contracts/agreements are of three types, viz., click-wrap, browse-wrap and shrink-wrap. The type of standard form of contract between these companies and its users is a *'click-wrap'* contract. A standard-form contract is prepared by one party, to be signed by the party in a weaker position, usually a consumer, who has little choice about the terms. Lord Diplock in *Schroeder Music Publishing Co. Ltd. v. Macaulay*[2] defined standard form contract as the one of modern origin, which have been dictated by parties with higher bargaining power, i.e., a *'take-it or leave-it'* contract.

The term "click-wrap" refers to electronic contracts requiring users to express their consent by clicking on an *"I accept"* button, or an equivalent, before completing their purchase, accessing the material they want to download or installing software they have purchased. Click-wrap agreements are standardized contracts whereby consumers assent to a set of terms and conditions. The three primary doctrines which the American courts use to review potential abuses in standard-form contracts are unconscionability; the reinstatement of contracts, and the doctrine of reasonable expectations. The word "unconscionable" means "showing no regard for conscience; irreconcilable with what is right or reasonable"[3].

Though the Indian Contract Act does not explicitly speak of 'unconscionability', Section 23 of the Act declares that no man can lawfully do that which is opposed to public policy.[4] Public policy is not capable of being given a precise definition; what is 'opposed to public policy' would be a matter depending upon the nature of the transaction.[5] In *Ramulu v. Director Tamil Nadu Refles*[6], the High Court of Madras held that, "if the terms of a contract are so unconscionable and if one of the terms is in terrorem and without any

[1] Ambarish Salodkar, Karan Morey and Prof. Mrs. Monali Shirbhate, "Electronic Wallet", International Research Journal of Engineering and Technology (IRJET), Volume 2, Issue 9, December 2019.
[2] Schroeder Music Publishing Co. Ltd. v. Macaulay, [1974] 1 WLR 1308.
[3] Robert A. Hillman, *The Richness of Contract Law: An Analysis and Critique of Contemporary Theories of Contract Law,* 129, 1997- explaining justification for, history, and application of unconscionability doctrine.
[4] Indian Contract Act, 1872. The Indian Contract Act, 1872, No. 9, Acts of Parliament, 1872, §23.
[5] State of Rajasthan v. Basant nahata, AIR 2005 SC 3401.
[6] Ramulu v. Director Tamil Nadu Refles, (1972) 2 MLJ 239.

consideration known to law, it would be in opposition to public policy and the party affected can approach the court for relief".

The ability of businesses to identify efficient allocation of risks also gives them the opportunity to exploit consumers by getting them to accept contract terms that inefficiently shift risks to consumers. Businesses understand the true risks of contracts better than consumers, and hence can include terms in the form that are much more favourable to them than consumers know or appreciate. In effect, businesses have incentives and opportunities both to allocate the risks of the contract efficiently and to impose hidden risks on consumers where possible.[7] Most commentators agree that only a tiny fraction of consumers read and understand boilerplate. Other factors therefore also must affect consumer behaviour. Social forces induce consumers to sign standard-form contracts quickly, even when they should take the time to read and understand them. Thus Indian courts have, since then, shown a marked willingness to interfere with printed form contracts where there is evidence of unequal bargaining power. It has been held that the courts would relieve the weaker party to a contract from unconscionable, oppressive, unfair, unjust and unconstitutional obligations in a standard form contract[8]. The Supreme Court has upheld a plea that a printed form contract was void on grounds of coercion, where the parties had unequal bargaining power.[9]

E-businesses present standard terms in a distinct take-it-or leave-it fashion. The terms are also long, detailed, full of legal jargon, about remote risks, and one-sided. Furthermore, consumers cannot negotiate because web pages and installation software do not allow for interaction with a live agent. E-consumers often cannot find answers to their questions about the terms. Courts recognize that standard-form transactions do not involve the required "bargain" of classical contract law.[10]

In India, the subject of unconscionability has been discussed by the Law Commission in the 103rd and 199th reports. The Law Commission of India in its 103rd Report suggested that an additional S.67A be added to the Indian

---

[7] Robert Lee Dickens, *Finding Common Ground in the World of Electronic Contracts: The Consistency of Legal Reasoning in Clickwrap Cases*, 412, 2007.

[8] Delhi Transport Corpn. v. DTC Mazdoor Congress, 1991 (1) SCC 600; Tata Chemicals v. Skypak Couriers, OP No. 66 of 1992; Lily White v. R. Munuswami, AIR 1966 Mad 13.

[9] R.S. Deboo v. Dr. M.V. Hindlekar, AIR 1995 Bom 68; Chairman and MD, NTPC Ltd. v. Reshmi Constructions, Builders and Contractors, (2004) 2 SCC 663.

[10] Thompson Crane & Trucking Co. v. Eyman, 267 P.2d 1043 (Cal. Dist. Ct. App. 1954), as instance where courts void contract terms that are not bargained for).

Contract Act, which is similar to the S.208 of the Restatement of Contracts[11]. The basic principle of the law of contract is "Freedom of contract". A person has the freedom to refuse to enter into a contract if either the terms of the contract or the party is not suitable to him. A Standard Form of Contract between the e-wallet companies and its users is voidable if its terms are invalid and dominant of privacy policy.

PRIVACY CONCERNS IN RECENT TIMES

Users of mobile wallets should be aware that their personal data is not safe anymore. Data is not just information but new era's weapon. The data of the users can be misused and can be used for various purposes. The recent Cambridge Analytica scandal has proved that data can be misused and it made Facebook guilty for its breach under UK of the Data Protection Act,[12] where it has been fined for £500,000, the maximum amount possible.

Whereas in India, there is no efficient solution for such offences. The law is still at its building stage on this grey area. Paytm, India's leading digital payments service, was in trouble after an investigative report allegedly showed a senior executive at Paytm claiming that the company had shared user data with the Prime Minister's Office (PMO).The recent revelations of Paytm's data privacy issue has lead to so many questions with regard to privacy concerns and data protection/privacy laws of India.[13] Cobrapost released a video as part of an exhaustive 'sting' operation dubbed 'Operation 136'.[14]

Internet Privacy could also be viewed as economically important since it gives consumers the assurance that their personal particulars will not be released to unauthorised persons. The Government of India has actually promoted the online transactions/cashless transactions by actually implementing demonetization. This move of the Government brings the responsibility on themselves to create a 'safe platform for the citizens'. This, in turn, would give consumers the confidence to participate more fully in e-commerce transactions. Moreover, the right to privacy is intimately connected with the freedom of expression and disregarding the right may lead to gross violations of the freedom of expression via the Internet[15]. The users' right to freedom of speech and expression under Article 19(1) (a)[16] of the Constitution

[11] Restatement of Contracts, 1979, Acts of USA, §208.
[12] Facebook fined for data breaches in Cambridge Analytica scandal, Alex Hern and David Pegg, 11th July, 2018.
[13] https://www.indiatoday.in/technology/talking-points/story/paytm-founder-vijay-shekhar-lost-private-data-and-almost-lost-rs-20-crore-you-don-t-make-such-mistakes-1373779-2018-10-23.
[14] https://www.androidauthority.com/did-indias-paytm-share-user-data-with-the-government-870102/
[15] N.R. Madhava Menon, *Computers Internet & E-Commerce*, 288, 4th ed, 2009.
[16] India Const. Art.19(1)(a).

is violated. Article 19 encompasses freedom of body as well as mind. "Privacy facilitates freedom and is intrinsic to the exercise of liberty"[17]. There lies a responsible duty on the State to protect fundamental rights of the citizens. Since right to privacy and right to freedom of expression are fundamental rights which are guaranteed under Part III of the Constitution, the state is obliged to safeguard the right to privacy of its citizens. The concerns on privacy arise in relation to confidentiality aspects between the data collector and individual's data. The entities collecting the information owe duty of care and duty to maintain confidentiality of such data, which extends from the collection of data to the deletion of data so collected.

In the case of *I v. State of Gujarat*[18], it was held that the State has a duty to protect those fundamental rights of the citizens conferred by the above mentioned Articles and if by any inaction or inadequate action, which is nothing but inaction, a person suffers for no fault on his part resulting in injury to his life and property including his data security, he can approach the High Court under Article 226 of the Constitution for appropriate remedy.[19]

Though, the Cyber Appellate tribunal exists to deal with such category of offences. The Government has diluted this particular institution by not providing adequate laws and appointments to it. The petitioner in *Vodafone Cellular v. UOI*[20] approached the Delhi High Court by way of a writ, as the Cyber Appellate Tribunal was not functioning, for over two years, as on the date of above petition. Based on the government's statement that the position was to be filled shortly, the Delhi High Court refused to intervene. The court did however, gave liberty to the petitioner to approach High Court, if the Cyber Appellate Tribunal was not functional within a reasonable period of time.[21]

INSUFFICIENT LAWS IN INDIA: COMPARATIVE ANALYSIS

The Laws of India are not on par with Data Protection Laws existing internationally. Privacy is an interest with several dimensions: One of these dimensions is the privacy of personal data, also known as "data privacy" or "information privacy". Privacy issues have only been addressed at the international levels and concerted international effort to protect individual privacy has begun. While the internet has been the impetus for instruments

[17] The Hansindia, *Understanding Right To Freedom*, http://www.Thehansindia.Com/Posts/Index/Civil-Services/2016-07-18/Understanding-Right-To-Freedom-Article-19-22/243045.
[18] I v. State of Gujarat, Special Civil Application No. 3023 of 2003.
[19] Id.
[20] Vodafone Cellular v. UOI, 2015 SCC Del 9348; Dhanalakshmi Bank Ltd v. Union of India, 2015 SCC Del 9360.
[21] N.S. Nappinai, *Technology Laws Decoded,* 575, 2017.

such as E.U. Data Protection Directive, countries such as India are still grappling with the basic concept of privacy and have barely touched upon the implications of internet on privacy specifically. [22]

In the United States, the legislation on privacy and data protection includes the Privacy Act[23], the Computer Fraud and Abuse Act[24] etc. The four core principles of privacy are notice/awareness principle, choice/consent principle, access/ participation principle and security/integration principle. The U.K. has a much more legalistic approach to protection of personal data in general. The Data Protection Act, 1998 lays down rules for processing personal information and applies to paper records as well as those held on computers.[25] Where as in India, there are only a few statutes which touch upon the subject of data privacy, viz., Information Technology Act, 2000; IT Rules, 2011, in scattered provisions.

A comparison with laws from other countries is worked here, to attribute appropriate protection to users' data and check upon where we stand while dealing with the apps that are functioning in India. On the other hand, protection of privacy rights during processing of data have not been stated in the objectives of the IT Act[26].

LACUNAE OF IT ACT

In Information Technology Act, 2000[27], the Sec. 72 deals with "Breach of Confidentiality and Privacy". It should be noted that this provision deals only with information collected by a person who secures the information in pursuance of powers that he or she exercises under the Act and doesn't cover in specific about the sensitive personal data. The liability of the entities is further diluted in Sec.79 by providing the criteria of "knowledge" and "best efforts" before determining the quantum of penalties. This means that the network service provider or an outsourcing service provider would not be liable for the breach of any third party data made available by him if he proves that the offence or contravention was committed without his knowledge, or that he had exercised all due diligence to prevent the commission of such offence or contravention.

---

[22] Yee Fen Lim, *Cyberspace Law: Commentaries And Materials*, 218, 2nd Ed, Oxford University Press, 2007.
[23] The Privacy Act, 1974, 5 U.S.C. § 552a.
[24] The Computer Fraud and Abuse Act, 1986 18 U.S.C. §1030.
[25] Nandan Kamath, *Law Relating To Computers, Internet And E-Commerce,* 313, 5th Ed, Universal Law Publishing Co,. 2000.
[26] Aditi Chaturvedi, *GDPR And India, The Center For Internet And Society*, India, at https://Cis-India.Org/Internet-Governance/Files/Gdpr-And-India.
[27] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, §72.

There is no express legislation in India dealing with data protection. Although the Personal Data Protection Bill was introduced in Parliament in 2006 and lapsed subsequently and recently also the draft is again modified and uploaded as The Personal Data Protection Bill, 2018,[28] it is yet to see the light of day. The bill seems to proceed on the general framework of the European Union Data Privacy Directive, 1996. It follows a comprehensive model which aims in governing the collection, processing and distribution of personal data. It is important to note that the applicability of the bill is limited to 'personal data' as defined in Clause 2 of the bill. If this bill would be passed as soon as possible, it would combat the data breaches to some extent at least. The citizens of this country are in dire need of this legislation.

Accessing data for law enforcement and criminal investigations should ideally be authorised by Courts of Law. Indian technology companies in the meantime need to be more transparent about the ways in which they share the data belonging to their users. This can be implemented in law enforcement guidelines, specifically providing the legal provisions that they respond to and the procedural requirements that they demand from law enforcement agencies. They should also publish transparency reports to make users aware of the total number of such requests that they receive and the numbers that they respond to.

CONCLUSION

The Committee of Experts on Data Protection Framework in India headed by Justice B.N. Srikrishna had released a draft paper on November 27, 2017. The Committee was constituted in August 2017 to examine issues related to data protection and recommend methods to address them, and draft a data protection law. The objective was to ensure growth of the digital economy while keeping personal data of citizens secure and protected. The Committee sought comments for certain questions raised by it till December 31, 2018. It will draft a law for data protection in India based on the feedback it receives. Very soon we could see the light of this statute and hope that it would curb the menace of data theft and make responsible third party companies in respect to people' personal data.

It would not be wrong to call 'Digital India' an envisaged mirage, if digitalization takes place without proper base and pillars. Countries like India need stringent legislations as pillars and active mechanism like base to deal the issues which arise out of the electronic wallet usage.

[28] Personal Data Protection Bill, 2018, (Dec 2nd, 8 PM) http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.

SECURING THE DIGITAL PAYMENT ECOSYSTEM: RISKS AND CHALLENGES

JP KAVI PRIYA*
&
RAMJI KUMAR

Abstract:

Traditionally, the field of payments has been bank driven. The DIGITAL INDIA mission by the Government of India, is aimed at transforming the country into Cashless and Digital economy. The phenomenal global growth in digital payments may be attributed to three factors – (i) Digital and technology revolution (ii) Entry of several non-banking PSPs (Payment Service Providers) into payments space and (iii) Customers becoming more demanding and expecting instantaneous and one-touch payment solutions. The speed at which the digital payment space is changing in India, we need to take a look on our cyber security public policies and regulations. Due to our contemporary evolution of digital payment ecosystem, changes in cyber security and data protection, for the end customer to have trust and confidence in this system, one requires a solid holistic cyber security framework covering regulatory and technological advancement.

The focus of this paper is to analyze the challenges of digital payments from different perspectives and provide preliminary security countermeasures for each of the issues. Finally, suggest recommendations that can be imperative for India to learn and adopt from global financial trends and technologies to align itself with global payment revolution. Since, cyber security preparedness for the digital payment space guarantees a concerted effort globally as per the 'vision 2018' document by RBI.

* JP KAVI PRIYA BBA. LLB (Hons), 4th year, SOEL and RAMJI KUMAR, BBA. LLB (Hons), 4th year, SOEL.

INTRODUCTION:-

It has been said that every disruption creates opportunities and one such disruption was the announcement of demonetization by Prime Minister Mr. Narendra Modi on 08th November 2016. Demonetization created huge growth opportunity for digital payment in India and the digital wallet companies grabbed the opportunities with both the hands to expand their market share.

Indian government and private sector companies such as Paytm, Freecharge and Mobikwik had been aggressively pushing several digital payment applications, including the Aadhaar Payment app, the UPI app, and the National Payments Corporation of India (NPCI) developed the Bharat Interface for Money (BHIM) app. Digital transfers using apps has brought behavioral change and helped in the adoption of digital payment.

The growth of India's cashless payment space is expected to be driven by four trends[1]:

- **Cash being expensive:** Though there are several perceived benefits of transacting cash (such as instantaneous settlement, relative anonymity, and the notion of security associated with holding physical value), there are several latent and implicit costs associated with cash.

- **Advancement in technology:** Technology has been advancing at a rapid pace to deliver robust, secure and convenient payments solutions. This enables rapid delivery of payment services to large sections of the population.

- **Economical:** Digital payments allow for services to be delivered at lower costs, afford greater scalability and greater ease of access. This in turn, helps fostering economic growth and financial inclusion.

[1] **Digital Payments: Challenges and Solutions,** Srihari Kulkarni, Abdul Shahanaz Taj, *IOSR Journal of Business and Management (IOSR-JBM) e-ISSN: 2278-487X, p-ISSN: 2319-7668 PP 50-55*

- **Government initiatives:** Initiatives taken by the government have created a catalytic environment for the greater proliferation and growth of digital payments. As and when there is a transition from nascent cashless economy to a mature one, we would witness a significant drop in cash based transaction. The transition in its course would however have its own share of pains for different stakeholders owing to overall structural changes that the system would encounter.

CHALLENGES OF CASHLESS TRANSACTION IN INDIA[2]:-

Some of the challenge which stands in the way of India becoming a cashless transaction are as

- ✓ **Cyber Security:** In October 2016, the details of over 30 lakh debit cards were feared to have been exposed at ATMs. Stringent steps issuing new cards were also taken such cyber-crimes are very dangerous while using the cashless transaction.
- ✓ **Network Connectivity:** To save that dreaded trip of standing in line to pay for a transaction at a shop and also due to an overload on the network of the card machines have stopped working. Connectivity issues must be resolved before dreaming about a cashless society.
- ✓ **Internet Cost:** The Internet cost in India is still substantially high. In order to convince people to do cashless transactions, the cost of the internet should be lowered.
- ✓ **Charges on Online Transactions through Cards:** Convenience charges are additional charges that are levied by the vendors when they offer an online payment facility, but the government is forcing people to go cashless. So charge on cards is a main problem in cashless transaction.
- ✓ **Non-Tech-Survey:** The new generation is glued to their phones and gadgets with computer literacy whereas many senior citizens are not aware of such technological aspects.

[2] Mobile Wallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures, Mansi Prakashbhai Bosamia, CMPICA, CHARUSAT.

- ✓ **Smart phone affordability:** Several companies have come up with new and inexpensive phones but still it remains unaffordable to majority of the population. More affordable options should be launched by the government for people.
- ✓ **Not Enough Bank Accounts:** many people still do not have bank accounts due to lack of banking knowledge which is one of the main problems of cashless transaction.
- ✓ **Internet Blockage:** States like Jammu and Kashmir often face crack down where the internet is the first thing that is blocked. In such situations neither is it possible to use cards for transactions nor is it possible to use of E-wallets.
- ✓ **Encourage People to Spend:** Spending by cards often encourages people to spend more. Not just through credit but even the debit cards give that impression that we can make that payment immediately.
- ✓ **Illiteracy:** One of the biggest problems which India is facing is illiteracy. Irony is that even some educated people, are unaware of the usage of computer and internet. So they are for away from Internet Banking.
- ✓ **Lacking infrastructure:** Retailers and consumers use swipe machines but they are not available on large scale. Customers have to wait in queue for long time for depositing cash in banks.

There has been significant improvement in all the above areas in the last 5 years. But we still have a long way to go before we can claim that we are part of Digital India.

RISKS IN THE ONLINE PAYMENT [3]:-

Users Risks

1. **Malware or Ransomware:** Users are unaware of malware infection in their devices. The malware is able to extract user credentials and share it with the adversaries. For example, according to last year's report by Kaspersky Labs, a new malware Xafecopy Trojan was

[3] ENISA, "Security of Mobile Payments & Digital Wallets," https://www.enisa.europa.eu/ publications/mobile-payments-security/at_download/full Report, 2016.

detected in India, which stole money through victims' mobile phones and it was cited that 40 % of this malware attacks were in India.

2. **Phishing and social engineering** are the most commonly used techniques to carry out cyber-attacks on the end users in the digital payment space. In phishing, deceptive link is sent to the user which appears legitimate and they are redirected to sites which belong to cyber adversaries. Also, adversaries may build **fraudulent wallet applications** and post it on the popular market places. There had been instances in which users transacted via illegitimate wallet applications instead of legitimate ones. The user without knowing about it transacts on it leading to loss of their credentials. Social engineers from unknown sources are navigating for opportunities either via telephonic conversations or well-crafted emails to cheat gullible users.
3. **Man-in-the-middle attack**. The communication layer of the transactions is vulnerable to cyber threats. In case of non-secure network implementation, adversaries are able to eavesdrop and fire a man-in- the-middle attack. With this method, they can change the data packets integrity or obtain key information to conduct frauds against users such as NFC based attack.

Platform Risks[4]

1. **Network Provider Threat:** When cyber attackers gain access to network provider it may compromise the end IT workforce. Adversaries may flood network providers leading to d**enial of services** as the functioning of the digital payment instruments, may deteriorate or resulting in non-availability of the prepaid payment instruments.
2. **Payment Application Provider threats:** A typical prepaid payment instrument consists of players such as payment application and infrastructure providers. The digital infrastructure of payment application provider ecosystem is to be protected against cyber threats.

[4] Security Aspects of Mobile Based E-Wallet International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 5, Issue: 6 ISSN: 2321-8169-1223 – 1228.

Crime-as-a-Service

Organized cyber gangs may be given a bounty by the adversaries to dupe end users transacting on the digital payment ecosystem. This may lead to many systematic organized crimes in the cyber space.

Impersonate Organizations

The current phishing techniques may get scaled in creating end-to-end fake online presence of the organizations to profit in billions, as users may fall prey to it.

Third Party

Organizations perimeters are getting blurred day-by-day, as more and more work is outsourced to third parties which is responsible to introduce new cyber threats into the core operational environment.

Malicious Insider

A disgruntled employee may cause havoc in an organization by stealing data, disrupting operations, inserting a backdoor in a financial services application or infrastructure based on the role he/she performs.

Attacks on two-factor authentication

Techniques such as SMS or Biometrics are being leveraged as second factor of authentication for carrying out digital payment transactions. In future, large scale social engineering attacks may be launched to obtain OTPs or unauthorized access into systems to steal biometrics of end users.

Hardware Vulnerabilities

Unmatched vulnerabilities of numerous hardware have leveraged in digital payment ecosystem to conduct frauds.

FUTURE RISKS:-

Mobile Malware Automation

With the use of advanced techniques such as machine learning and Artificial Intelligence (AI), adversaries are developing malwares which can infect user devices surreptitiously in an automated way, with no human intervention.

Cyber Warfare/Espionage

Nations are leveraging cyberspace as ground for cyber war; it may impact functioning of digital payment infrastructure at large. Adversaries breaching organizations IT boundaries to steal corporate or R&D secrets, resulting in cyber espionage

Misuse of emerging technologies and platform

1. **National Unique ID Ubiquity**: Mandating National Unique ID linking with every service in India may expand the user threat surface, as adversaries may get enticed to break into financial systems via National Unique ID.
2. **IoT Attacks**: Users of digital payments are adopting wearable's such as smart watches to conduct commerce. These wearable devices are vulnerable to cyber threats such as acting as botnets in which they are used to conduct denial of services attacks without user knowledge.
3. **Social Media Attacks**: Social media integration with digital payments is getting prevalent where login into payment applications using social media ID leading to **avatar hijacking** from current identity thefts. The adversaries may be able to clone an illegitimate digital avatar of the user. Organizations may not be in a position to distinguish between real and fake avatars of the users.
4. **Advanced Technology Attacks**: Techniques such as artificial intelligence, machine learning and deep learning may increase complexities of cyber-attacks and may automate them with minimum human intervention.

5. **Crypto currency**: Ransom demanded in crypto currencies which are untraceable may propel rise of cyber-attacks on financial services and its users, with more motivation.

Complexities in Digital Payment Infrastructure:

With implementation of technology advancement in the products, integrating multiple services or components which may result in mesh of IT architecture, this may result in uncovered vulnerabilities in the system leading to cyber incidents.

SECURING SECURITY IN CASHLESS ECONOMY[5]:-

1. **Agile security practices:** Security in this context can no longer be a standalone post-facto toll gate. Security assessment and **testing will need to be embedded into the agile development life cycle.** Agile security testing methods based on **automation will have to be adopted**. In many ways, a paradigm shift is needed in the way security testing is undertaken today.

2. **Securing the hyper-interfaced environment:** With faster proliferation of interfaces, **protecting APIs will become critical to ensure malware and persistent threats do not propagate** through such untrusted / untested APIs.

3. **Next generation authentication: Adaptive authentication will need to be embedded into the heart of transaction** processing. Next generation authentication will use triangulation techniques while considering larger data sets including the nature of transaction, merchant type and transaction channel.

4. **Protecting context-rich personally identifiable information (PII):** The new generation data marts will not be limited to traditional transactions and account-related information but will have enriched **data** insights such as spending patterns, patterns of digital platform usage, preferences and other person-specific information sets. In an integrated ecosystem, such data sets may be stored, transferred or

[5] Securing the cashless economy, ASSOCHAM India.

shared with third parties for revenue generation opportunities. Both regulators and organizations will be obligated to invest in strong processes and technology to prevent the misuse of context-driven rich PII. While traditional controls such as data masking and encryption will need to be enhanced, capabilities to hunt down any misuse of PII will have to be built by organizations.

5. **Security of the new perimeter - mobility:** In the new digital/cashless economy, mobility-based solutions will continue to gain prominence and, hence, security concerns will no longer be limited to the organization architecture boundaries. Mobility will form a new perimeter of the organization. In order to ensure an endpoint, security containerized apps with built-in advanced persistent threat (APT) capabilities will have to be developed. Hence, the next generation financial infrastructure may involve the adoption of advanced end-user device management solutions.

6. **High velocity identification, containment and eradication:** In today's life every consumer is using multiple platforms and services across the ecosystem. Any threat that impacts such user can potentially proliferate and bring the entire financial services ecosystem to a standstill. As the ecosystem continues to be interconnected and overlapping, cybercriminals will try to exploit possible lapses and, hence, strategies need to be built to deal with such eventualities. Given this interdependence on all the players of the financial ecosystem, it becomes crucial to identify any anomaly at a pace which mirrors real time or near real time.

7. **Augmented ecosystem control:** The new age enterprises will adopt the cloud for faster roll-out and to address non-linear growth. The security boundaries of the various players will be extended to end users, third parties and other ecosystem partners. The process for monitoring of parameters will also have to be integrated with the company's incident response framework.

8. **Ubiquitous awareness:** The cashless economy means that the stakeholder community will now not just be limited to internal stakeholders but will also include external as well as peripheral

stakeholders (like merchants).With the influx of first-time users, users from various linguistic ethnic groups and users of different channels, the soft targets will be multifold. The awareness theme for tomorrow will thus be multichannel, multilingual and multicultural, and hence go beyond the scope of traditional programmers.

REGULATIONS AND POLICY PRESENT IN LAW:-

(I) RBI MASTER DIRECTIONS ON ISSUANCE AND OPERATION OF PREPAID PAYMENT INSTRUMENTS IN INDIA[6].

- Section 15 stipulates security, fraud and risk management framework; Section 16 covers customer protection and grievance redressed framework and Section 17 entails system audit requirements.
- Adequate information and data security infrastructure and systems for prevention and detection of frauds to be implemented by the PPIs with an emphasis on strong risk management system.
- Requirement on a formal, publicly disclosed customer grievance redressal framework. PPI issuers shall create sufficient awareness and educate customers in the secure use of the PPIs and Report the frauds on a monthly / quarterly basis to the concerned RBI Regional Offices.
- Establish a mechanism for monitoring, handling and follow-up of cyber security incidents and cyber security breaches. This is to be in place for reporting incidents to RBI & CERT-In.
- Board approved information security policy and best practices on restricting multiple invalid attempts on account, velocity check on number of transactions, internal and external escalation mechanisms, MIS systems security, inactivity timeout failures, etc.
- Process of determining customer liability in case of unauthorized / fraudulent transactions involving PPIs.

[6] RBI, "Master Direction on Issuance and Operation of Prepaid Payment Instruments," https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11142, 2017.

- Minimum baseline requirements such as mobile app not to be installed on rooted or jail broken devices, source code audit, integrated SoC Model, subscription to anti-phishing/anti-rouge app services, disaster recovery services, etc.

ANALYSIS:-

Mandatory security requirements from the regulator which is to be adhered by online payment instruments organizations in India. This may enable trust in digital payment space for users to adopt digital payment channels at mass scale.

The requirements also provide a framework for the end users to submit their grievances and ensure protection of their transactions.

(II) DRAFT MEITY SECURITY RULES FOR PREPAID PAYMENT INSTRUMENTS[7]

- Mandates following process requirements such as, but not limited to, information security policy, privacy policy, and risk assessment, reporting of incidents, grievance redressal and adherence to security standards to be stipulated by Meity.
- Stipulate technological requirements such as, but not limited to, security of personal information, access to personal information, end-to-end encryption, traceability, retention of information, customer identification and authentication, etc.

Analysis:-

Mandatory prescriptive security requirements from the ministry which is to be adhered by online payment instrument organizations in India. If stipulated, this may add to compliance burden and may impact the innovation space in digital payment ecosystem.

(III) MEDIUM TERM RECOMMENDATIONS TO STRENGTHEN DIGITAL PAYMENTS ECOSYSTEM, WATAL COMMITTEE REPORT[8]

[7] Meity, "Draft Meity Security Rules for Prepaid Payment Instruments," http://meity.gov.in/writereaddata/files/draft-rules-security%20of%20PPI-for%20public%20comments.pdf, 2017.

- Make regulation of payments independent from the function of central banking.
- Update the current Payments and Settlement Systems Act, 2007 to include explicit mandate for consumer protection including penalties and independent appeal mechanism, regulations on systemic risks, data protection and security and a process of regulatory governance.

Analysis:-

It consists of holistic recommendations from finance ministry committee to provide direction for overall digital payment space in India. It clearly articulates the importance of cyber Security to propel digital Payment adoption.

REGULATION AND POLICY NEEDED IN FUTURE:-

(I) DATA PRIVACY LAW[9] - 2019

The Indian Government has appointed an expert committee, headed by former Supreme Court judge BN Srikrishna, to build visibility on key issues with respect to data protection and to provide recommendation. This may result in data privacy regulation for India.

Analysis:-

- The major outcome of this committee's activities may be an enactment of a data protection law in India. The stipulations in it which are work-in- progress may cover areas such as, but not limited to, notice, choice, consent, usage limitation, stand on data localization, privacy policies, securing data, need of privacy impact assessment and protecting Indian citizen's fundamental right to privacy.
- These new compliance requirements of future from data protection aspect may impact how organizations may build digital payment

[8] Ministry of Finance, "Watal Report on Digital Payments," http://mof.gov.in/reports/watal_ report271216.pdf, 2016.
[9] Meity, "Data Privacy Law of India," http://pib.nic.in/newsite/PrintRelease.aspx?relid=169420, 2017.

infrastructure and products to operate in this space. The future data protection law may also act as an enabler for end user to adopt digital payments with enhanced confidence and trust; as it is expected to provide assurance and grievance framework for the end citizens.

(II) RBI DIGITAL PAYMENT SECURITY SUB-COMMITTEES-2019

The **First Sub-Committee** is on "Mobile Banking and Security". It is studying various global security standards and protocols. The end outcome is to table best practices for mobile security for trusted banking (an enabler for digital payments in India) and promote its adoption across organizations in the country. Also to identify authorities/institutions/stakeholder(s) in the mobile financial ecosystem that are in the best position to implement the measures as to be stipulated in the cyber security best practices report.

The **Second Sub-Committee** is on "Card Based Payment and Security". This sub-committee is mandated to examine best practices in securing card based payments, identify gaps in current regulatory ecosystem, study the threats and solutions for PoS machines, compliance with extant standards, etc.

Analysis:-

- The sub-committee's activities may result in cyber security guidelines on mobile banking and card payments. This can be a good start for digital payment organizations to understand regulator viewpoint from best practices implementation aspect.
- Detailed guidelines from regulators prepared in consultation with industry helps organizations in building trust with end customers.

(III) PROTOCOL FOR E-WALLET COMPANIES[10]-2020

[10] Economic Times, "Protocol for e-Wallet Companies," http://cio.economictimes.indiatimes.com/news/digital-security/government-plans-norms-for-e-wallet-firms-to-prevent-onlinefrauds/60774069, 2017.

The Government of India is in discussion stage to explore stipulation of standard protocol for e-wallet companies, so as to prevent and fight online financial frauds, in the advent of rise of digital payment space and associated cyber threats. It is also speculated that the government is exploring to formulate a 'Digital Payments Act' to regulate e-payments.

Analysis:-

Government stipulating a 'Digital Payment Act', may also include cyber security requirements for digital payment organizations. At the same time, a dedicated holistic regulation which is to be supported by RBI master directions and data protection law of future may act as a factor of trust to propel digital payment adoption.

(IV) GLOBAL CHALLENGE FOR CYBER SECURITY WORKFORCE-2019[11]

The Ministry of Electronics and IT in collaboration with Cyber Peace Foundation (CPF) is planning to organize a global cyber challenge. The government's digital platform 'Mygov' has invited people to participate. The primary objective is to elevate the domain of cyber security; the challenge is to be based on numerous problem statements and participants may propose solutions resulting in an application or a product.

Analysis:-

Challenge similar to this on national level helps building capacity and capabilities in the realm of cyber security. Evolution of capabilities and skill building with the help of global platforms like these puts India, to lead from front in securing digital payment space globally. This challenge can also benefit the space of digital payment security, as new protection solutions may emerge and it augments the skill building agenda of the country in the domain of cyber security.

(V) ESTABLISHMENT OF FINANCIAL CERT, INDIA[12] - 2018-2019.

[11] Indian Express, "Global Challenge for Cyber Security Workforce," http://www.newindianexpress.com/nation/2017/oct/07/government-to-hold-global-challenge-to-build-cyber-taskforce-forindia-1668336.html , 2017.

An expert group has proposed the setting up of an independent Computer Emergency Response Team for Finance (CERT-Fin) to be the cyber warrior of the financial sector.

Analysis:-

CERT-Fin will be the key to ensuring a comprehensive cyber security framework for the financial sector, especially at a time when there has been a burst of activity in the Fintech space as India makes efforts to embrace a less-cash economy.

CONCLUSION:-

In conclusion, cyber security will continue to be a type of asymmetric warfare:

Each organisation will face a multitude of cyber adversaries, and their ranks will grow and become more sophisticated. The new reality is that cyber attackers are sufficiently capable and motivated to break through the defences. Hence, organisations will have to develop novel preventive control mechanisms and significantly invest in reactive capabilities. We believe mastering the areas highlighted above will help financial services companies reach the forefront of the industry. This is because incorporating a more agile cyber risk management approach may enable them to more effectively harness the ongoing digital revolution to their advantage.

[12] I. Ministry of Finance, "Financial Cert," http://dea.gov.in/sites/default/files/Press-CERT-Fin%20 Report.pdf, 2017.

SECURITY STANDARDS OF E-WALLETS UNDER INDIAN LAWS: ISSUES AND CHALLENGES

Anithaa Selvi B*

Abstract

At the dawn of the 21st century with the rising technological innovations and advancements, the Indian economy is striving towards active digital transactions throughout the country. With the popularization of cashless transactions especially after demonetization, people are now inclined towards e-wallets on account of its convenience and accessibility. While cashless transactions are being regarded as the future, there arises a need to address the security and privacy issues that need to be overcome for the success of digital payments. With a ton of security perspectives that are still left unexplored, security standards have to be laid to facilitate more secure transactions. The Information Technology Act, 2000, Payment and Settlements Act, 2007 and the RBI Guidelines govern the laws and policies relating to digital transactions. Drawing attention to e-wallets, there is no stringent and specific framework of the security standards. In reality, there is low compliance to the Information Technology Act, 2000 by large companies and there are possible risks of companies cloaking under the Terms & Conditions in order to bind the consumers and leave them in jeopardy. This paper seeks to analyse the laws and guidelines applicable to e-wallets and the challenges that are needed to be overcome for moving towards a cashless society.

1. Introduction

The rapid increase in the growth of e-commerce market today have brought e-wallets to the centre stage especially after the 2016 Indian banknote demonetization period that hit the country like a storm.[1] In order to cope up with the effects of demonetization, India majorly started resorting to cashless transactions that resulted in the

* 3rd Year, B.A.LL.B. (Hons.) Student at the Tamil Nadu National Law University, Tiruchirappalli.

[1] Javed Anwer, *After demonetisation, e-wallets strike it rich while India runs out of cash,* India Today, November 23, 2016, https://www.indiatoday.in/technology/features/story/after-demonetisation-e-wallets-strike-it-rich-while-india-runs-out-of-cash-353575-2016-11-23, <last accessed on 18.12.2018>.

rise of e-wallets in the Indian scenario as it forced merchants to look for alternatives. The e-wallet user base almost doubled in less than a year to overcome this 'war on cash' by the State itself.[2] This after-effect has led to a promising future and possibilities along with the rise in technological innovations and advancements. The traditional methods of payments through banks are now getting replaced with internet based payment systems as it has provided people with ease and convenience of accessibility paving way to the popularity of e-wallets. While enjoying the benefits of e-wallets, it is necessary to look into the security implications of online transactions and digital payments through e-wallets. India is among the top nations that are vulnerable to cyber attacks which were concluded after identifying the cyber security policies. The wallets and online mobile banking applications in India do not use hardware level security as said by Qualcomm which is making it more vulnerable to attacks.[3] When such is the case, the passwords can be stolen through capturing the fingerprints of the users. As the current legal framework is very limited for online payments, it is necessary for a strong legal framework to protect the data of the people as there is more exposure to risks with the widespread use and reliance on e-wallets such as PayTM, MobiKwik and FreeCharge. The future of these electronic payments is not confined to only its ease and accessibility but also on how it overcomes the issues of law and security standards so as to make it to be practically viable. Thereby, this paper seeks to analyse the current legal framework with regard to the security standards of e-wallets and secondly, the issues that are present and the need to overcome the challenges.

2. Laws applicable to e-wallets

Currently, there is no specific legislation for the data protection and security under Indian law. In 2013, the Ministry for Electronics and

[2] Payel Naiya, *Mobile Leading The Way: Wallet Payments Almost Double in One Year in India,* Counterpoint, November 8, 2017, https://www.counterpointresearch.com/mobile-leading-the-way-wallet-payments-almost-double-in-one-year-in-india/, <last accessed on 17.12.2018>.

[3] Mohul Ghosh, *Qualcomm Claims All Indian E-Wallets Are Insecure, Prone To Hacks; Pushes For Hardware Based Security Layer,* Trak.in, March 9, 2018, https://trak.in/tags/business/2016/12/14/indian-digital-mobile-wallets-insecure-hack-prone-qualcomm/, <last accessed on 18.12.18>

Information Technology released a National Cyber security Policy.[4] Though it highlighted the need for a specific legislation to ensure security and data protection, there is no such legislation dedicated to ensure the same. However, there are two legal frameworks that are applicable to e-wallets for the security under which the RBI issues circulars and guidelines that are the Information and Technology Act, 2000, and Payment and Settlement Systems Act, 2007.

2.1. Information Technology Act, 2000

In case of a customer being subject to any fraud due to e-wallets, the first measure that the victim should take is to inform the bank through which the e-wallet account is linked, after which a detailed complaint is to be filed with the online fraud cells run by the cyber crime unit. In furtherance to this, a written complaint to the bank, mobile service provider, e-wallet company, and any other third party vender who is related with the fraud is to be filed.

In the absence of any effective steps by the complaint redressal mechanism, legal route is the only recourse to the victim. Here arises the question as to whether there is any effective mechanism to avail a legal remedy. The Master Circular published by the RBI for online payment instruments enlist protective measures for e-wallet customers.[5] The RBI has made rules and guidelines for the minimum capital requirement or deployment of money collected and emphazised on the need of the establishment and functioning of the grievance redressal cells. In order to maintain proper security it is necessary for the e-wallet provider to guarantee that the app is not applicable on rooted devices and a pre-check is to be conducted regarding any malicious codes on the app before launching it.

Even though there are guidelines issued by the RBI, the guidelines only ask for the e-wallet provider to take "adequate" measures for safety and data security in order to prevent frauds. In

[4] National Cyber Security Policy-2013, Ministry of Electronics & Information Technology, Government of India, http://meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf <last accessed on 18.12.18>

[5] Master Direction DPSS.CO.PD.No.1164/02.14.006/2017-18, Master Direction on Issuance and Operation of Prepaid Payment Instruments, Reserve Bank of India, December 29, 2017, https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11142, <last accessed on 17.12.18>

case the RBI guidelines do not provide for any recourse, then Section 43 A of the Information Technology Act, 2000 which deals with the security of the information held by the private companies is applicable. It mandates the e-wallet provider to maintain 'reasonable security practices and procedures'. Under Section 43A, IT Sensitive Personal Data Rules, 2011, it was issued that require the e-wallet provider to have security practices proportionate to the data in possession. Failure to adherence to the same, the e-wallet provider has to compensate the victim without any upper limit for compensation being provided in the rules.

2.2. Payment and Settlement Systems Act, 2007

The Payment and Settlement Systems Act, 2007 deals with regulatory aspects pertaining to payment systems in India. Section 18 of the Payment and Settlement, 2007 provides RBI with the power to give directions and lays down policies for the regulation of payment systems that affect domestic transactions. Section 10(2) provides RBI with the power to determine standards for the management of specific payment systems. In lieu of this, RBI has been issuing circulars and Master Direction on Issuance and Operation of Prepaid Payment Instruments. There are three types of payment instruments namely closed system payment instruments, semi-closed system payment instruments and open system payment instruments. According to the RBI circular under the Act, semi-closed system payment instruments constitute the e-wallets that can be used for purchasing goods and services including services from merchants or establishments which are in a contractual relationship with the issuer to use the payment instrument as a medium for transactions.

Section 38 of the Payments and Settlement Systems Act, 2007 provides the RBI with the power to formulate regulations under which the Payments and Settlement Systems Regulations, 2008 is conferred with the powers.[6] In order to set up a payment system, any entity must adhere to the Payment and Settlement Systems Regulations, 2008. If

[6] Payment and Settlement Systems Regulations, 2008 (As amended January 2017), Reserve Bank of India, December 20,2017, https://rbi.org.in/Scripts/OccasionalPublications.aspx?head=Payment%20and%20Settlement%20Systems%20Regulations,%202008 <last accessed on 18.12.18>

the applicant complies with the provisions upon the satisfaction of the RBI, then the RBI issues an authorization certificate for the setting up of the payment system. The RBI can also refuse the application.

In 2016, the RBI released a comprehensive cyber security framework to regulate banks. Along the same line, the RBI released a notification under Section 10(2) of the Payment and Settlement Systems Act, 2007 addressing the "Security and Risk Mitigation Measures" specifically for prepaid instrument issuers after it had acknowledged the need for adequate cyber security for the dream of a cashless society to become successful. It advises the issuers of prepaid instruments to take appropriate steps to take "adequate measures" for the safe security practices and to protect people from being victims to phishing attacks. Also it has been made necessary to take dynamic measures in order to keep them in place.

3. Issues and Challenges

E-wallets are prone to several online fraud and theft such as identity theft, SIM swap, phishing attacks, brute force, malware, vulnerable payment technology and ransomware.[7] By connecting to open Wi-Fi networks and accessing mails containing viruses, people fall prey to getting their personal data stolen as it makes hacking easier to gain access to the account of the user leading to identity theft. E-wallets work mostly relying on one-time passwords for the safety of the user. This is also in threat as fraudsters purchase duplicate SIM with fake ID by gaining the credentials of the user, and in turn generate one time passwords to access the account of the e-wallet user. Usage of advanced hacking systems is prevalent worldwide that make payment technology vulnerable to risks by cybercriminals.

The issue with Section 43A of the Information Technology Act to govern e-wallets is that the liability of the e-wallet company ends once the company proves that they have maintained the security standard that are reasonable and adequate. In reality, it is shown that the compliance with Section 43A by the companies is very minimal as they

[7] Priyadarshini Maji, *Web of Frauds,* Business Today, January 22, 2017, https://www.businesstoday.in/magazine/money-today/investment/web-of-frauds/story/243774.html <last accessed on 18.12.18>

do not even practically apply the security standards that are merely documented.

Furthermore, Section 43A of the IT Act allows the e-wallet service provider to enter into agreements with the user to determine the security practices and procedures to make them adequate. For example, the stipulations in the Terms and Conditions make the user binding and provide the user with assured highest protection via the Terms and Conditions. The problem that arises with this is that there is no verification provided in the law for the compliance with the security as assured.

In addition to this, the e-wallet providers do not provide any liability for the security of data or bugs in the software. It is not clearly available as to find which is binding when there is any fraud or breach as the IT Act provides for the need for adequate security standards whereas the e-wallet provider is allowed to set the security standards. In case of any fraud or dispute and when the standards set by the e-wallet provider are inadequate, it is not clear as to which would prevail for recourse. It is also possible for the e-wallet service providing company holding customers through the Terms and Conditions without having adequate standards. It is necessary for the law to step up with this regard, especially when people are ignorant with the role of the security requirements for safe transactions.

There is a need to have fixed security standards as people are increasingly opting to e-wallets. It is very much important to establish a method to verify the compliance of the corporations with the rules to be enshrined under Section 43A as it lacks the same. It would be more adequate if there are laws that establish the rights and liabilities of the users as well as the corporations so that both of them are protected. In order to move to a cashless society, laws are necessary.

Security and fraud risks are of great concern and are a challenge to the adoption by the consumers to which we shouldn't turn our backs to. In order to prevent financial loss and damage, it is necessary to keep technology secure. It becomes necessary to have cost effective measures to overcome the risks that are prevalent because of the mobile payments. Pertaining to security, it is necessary to have network

security, application security, vulnerability threat management and device security.[8]

Most foreign countries that provide e-wallet services use hardware based security layer to make them less prone to risks and to secure them that are not used by any of the e-wallet service providers in India. The increase of demand of these e-wallets must be met with maximum security and not mere fingerprint sensors and app passwords that are vulnerable to theft. The policies and procedures by the government in order to keep the risk management in check have to be monitored as to whether there is compliance to it with more specific measures for security. Vague terms such as mandating "adequate measures" make it easy for the e-wallet providers to establish their applications without any appropriate measure for utmost security. It is necessary to have privacy impact assessments to identify and manage information from any risks of privacy associated with e-wallets and mobile payments. Data management to understand the risk associated with data sets to incorporate appropriate data governance and mechanism to gain benefit from the data within a secure framework. It is also necessary to develop mechanisms to support and comply with the regulatory requirements without an attitude to escape the laws. The e-wallet providers must have plans to control or provide with remedies in case of vulnerabilities in the process of mobile payments.

4. Conclusion

In the absence of minimum standards of security by the Indian law other than the RBI's Master Circular on Pre-Paid Payment Instruments that only provides with eligibility criteria, it is necessary to have a minimum standard to which it needs adherence to. In the absence of any such minimum security standards, millions of e-wallet users have been exposed to cyber crimes. The risk of digital fraud has increased along with the need for digital payments in the e-wallet era as hackers are attracted towards the current scenario considering the demonetization move by the government. The effective solution to this is to have standard security procedures that are

[8] Rajneesh Mishra, Mobile Application Security Building security into the development process, SDGC, https://www.sdgc.com/sites/default/files/pdfs/mobile_applicaton_security_wp.pdf <last accessed on 18.12.18>

unanimously adhered to by the e-wallet providers. This could ensure security and encryption measures across wallets. Information that is absolutely necessary for the prevention of frauds is to be collected, and not the ones leading to identification of the customer that invade the privacy of the customer. Measures like connecting to the KYC details must be within the framework that the regulations mandate. Thus, when the problem of security is being overcome, then that would invariably strengthen the e-wallet regime in the country to achieve a cashless society.

References:

- Abhay Upadhayaya, *Electronic Commerce and E-wallet,* International Journal of Recent Research and Review, Volume 1, March 2012, ISSN 2277 – 8322.
- DR.S.Manikandan, and J.Mary Jayakodi., *An Emprical Study on Consumers Adoption of Mobile Wallet with Special Reference to Chennai City,* International Journal of Research - Granthaalayah, 5(5), 107-115. https://doi.org/10.5281/zenodo.583902.
- G. Udhayaraj, D. Jocil, *A study on Electronic Payment System- E-WALLET* International Journal of Emerging Technology in Computer Science & Electronics, Volume 24 Issue 3, February 2017.
- G.Kanimozhi, K.S. Kamatchi, *Security Aspects of Mobile Based E-Wallet,* International Journal on Recent and Innovation Trends in Computing and Communication, Volume 5 Issue 6, June 2017, ISSN 2321-8169, available at www.irjritcc.org
- Information Technology Act, 2000.
- Madhu Chauhan, Isha Shingari, *Future of e-Wallets: A Perspective From Under Graduates',* International Journals of Advanced Research in Computer Science and Software Engineering, Volume 7 Issue 8, August 2017, ISSN 2277-128X.
- Master Direction DPSS.CO.PD.No.1164/02.14.006/2017-18, Master Direction on Issuance and Operation of Prepaid Payment Instruments, Reserve Bank of India, December 29, 2017, https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11142
- Payment and Settlement Systems Act, 2007.

- Payment and Settlement Systems Regulations, 2008 (As amended January 2017), Reserve Bank of India, December 20, 2017, https://rbi.org.in/Scripts/OccasionalPublications.aspx?head=Payment%20and%20Settlement%20Systems%20Regulations,%202008
- Rajneesh Mishra, Mobile Application Security Building security into the development process, SDGC, https://www.sdgc.com/sites/default/files/pdfs/mobile_applicaton_security_wp.pdf.

Section-III

Grievance Redressal Mechanism in the Banking Sector

GRIEVANCE REDRESSAL MECHANISM IN BANKS

SANJAY PINTO*

Preamble:

'Lopsided.' That defines banking practices in India. Despite periodic Circulars and Regulations of the RBI, and the Banking Regulation Act, 1949, the grievance redressal mechanism is characterised by robotic template responses to complaints and a farce of 'Relationship Managers'. The Banking Ombudsman Scheme, 2006, amended in 2017, also seldom provides relief to consumers, denting their faith in this avenue of redressal and triggering a proliferation of consumer cases for 'deficiency in service' and 'unfair trade practices' under Sections 2(1)(g) and 2(1)(r) of the Consumer Protection Act. This paper critically evaluates the existing two – tier system of grievance redressal – at the respective banks and by the Banking Ombudsman, shines a bright light on the most common grievances of customers and concludes that the resolution mechanism is porous, grossly inadequate and in dire need of an overhaul.

Robotic responses to grievances:

There was a time when the Branch Manager of Banks used to have an almost ubiquitous presence, have a personal rapport with customers and nip grievances even before they bud. With honourable exceptions, in many banks they are out on work or too immersed with their targets that the ordinary customer gets no immediate attention to his woes. An oral complaint is seldom taken seriously, an email elicits a reference number and a template response with no application of mind. Ditto with issues raised to the twitter handles and facebook accounts of banks. Complaints are trivialised as 'feedback' or 'concerns'. Many 24 hour helplines seem programmed to just parrot complaint numbers with no understanding of the issue communicated and may end up as an unintended cure for low blood pressure! What could have been solved in a jiffy is allowed to fester.

Customers run out of patience and their plight worsens.

* Advocate – Madras High Court, Columnist, Author & Former Resident Editor – NDTV 24x7

'RELATIONSHIP' MANAGERS: MARKETING RESOURCES CAMOUFLAGED AS TROUBLESHOOTERS

A sense of importance initially envelops the mind of customers, especially of private MNC banks, when they reach the 'exalted' position of being assigned a 'Relationship Manager'. The legitimate expectation would be assistance in a time of need – like blocking a lost card or getting a demand draft urgently or helping with queries like the status of deposited cheques. The bubble bursts with a loud thud when customers actually attempt to reach out to these designated officers in a crisis or to resolve grievances. Quite contrary to their impression that the Relationship Manager would have customer numbers on their speed dial, enquiries reveal that such officials are assigned to hundreds of customers! There is no exclusivity or a chosen few in a group. It's a wide net cast by banks to make customers feel special and to open a channel of marketing, which would otherwise not be entertained. The legal maxim "you cannot do indirectly what you cannot do directly" applies squarely to this deceptive practice by banks, as they try to sell credit cards, loans and a slew of financial products through an essentially marketing resource, camouflaged as a grievance redressal mechanism.

BANKING OMBUDSMEN: ADJUDICATORS IN THEIR OWN CAUSE?

Birds of a feather adjudicate together! If your complaint to your bank does not elicit a satisfactory response in a month, you can approach the Banking Ombudsman, not later than one year. But who exactly is this exalted authority? Under clause 4(1) of the Banking Ombudsman Scheme, 2006, emanating from Section 35A of the Banking

Regulation Act, 1949, he is an official of the Reserve Bank of India in the rank of Chief General Manager or General Manager. How fair is it to allow bank officials to be judges in their own cause? It would be naive to expect them to not lean in favour of their industry.

The **Supreme Court in Durga Hotel Complex Vs. Reserve Bank of India**[1] had observed that *"conceptually, an Ombudsman is only a non-adversarial adjudicator of disputes. He is an independent and non-*

[1] https://indiankanoon.org/doc/1620588/

partisan officer who deals with specific complaints from the public against administrative injustice and maladministration." However, realistically, how does the ombudsman work on the ground?

Hold your breath. The **Reserve Bank of India's Annual Report on the Banking Ombudsman Scheme, 2016-17**[2], reveals that awards were passed by ombudsmen in 0.05% of complaints filed by bank customers. That's a measly 65 awards out of the 1.3 lakh complaints received by the Ombudsman in 2016-17. There's more. More than half the maintainable complaints, a staggering 57%, were rejected. This is probably indicative of procedural challenges. Strangely, under clause 9(1) a complaint can be made to the ombudsman by a customer or his authorised representative "other than an advocate". The bar on lawyers appearing before ombudsmen places customers at a disadvantage, resulting in a proliferation of cases before consumer fora.

In keeping with the maxim that *'justice must also be seen to be done'*, why should ombudsmen be only bank officials? Why can't they be drawn from relevant fields – law, finance, media, judiciary or NGOs? If an RBI Governor can be a generalist, why can't ombudsmen be from other professions?

In 2014, the RBI came up with a **Charter of Customer Rights**[3]**.** It enshrined broad overarching principles for the protection of bank customers through five basic rights - Right to Fair Treatment, Right to Transparency, Fair and Honest Dealing, Right to Suitability, Right to Privacy and Right to Grievance Redressal and Compensation.

The RBI amended the Banking Ombudsman Scheme in 2017[4]. With effect from the July, 2017, the scope has been enlarged to bring within its ambit, deficiencies arising out of the sale of insurance, mutual funds and other third party investment products by banks. Customers can now lodge complaints against banks for non-adherence to RBI instructions on Mobile Banking/Electronic Banking services in India. The pecuniary jurisdiction of the Banking Ombudsman to pass

[2] https://rbidocs.rbi.org.in/rdocs/AnnualReport/PDFs/RBIAR201617_FE1DA2F97D61249B1B21C4EA66250841F.PDF
[3] https://rbidocs.rbi.org.in/rdocs/content/pdfs/CCSR03122014_1.pdf
[4] https://rbidocs.rbi.org.in/rdocs/Content/PDFs/BOS2006_2302017.pdf

an Award has been doubled to 20 lakh rupees. Compensation not exceeding two lakh rupees can also be awarded by the Ombudsman to complainants for loss of time, expenses incurred, harassment and mental agony.

Even after the 2017 amendments, it appears that banks still stick to technicalities. The **Chattisgarh State Consumer Disputes Redressal Commission in Shakti Bricks Vs. Branch Manager, Central Bank Of India**[5] pointed out that the Consumer Protection Act provides an additional remedy and under Section 3, it clearly stipulates that it is not in derogation of any other law. So not exhausting the ombudsman route is no bar to a consumer complaint.

Have ombudsmen become less rigid? The **Uttarakhand State Commission in Pulak Raj Mullick Vs Punjab National Bank**[6] noted that the "Banking Ombudsman without granting any personal hearing summarily dismissed the complaint with a finding that since the complaint requires detailed investigations and oral evidences, the complainant can approach any other appropriate forum or Court for redressal of his grievance."

There are about 30 grounds to file a complaint before the ombudsman in the amended scheme. But the list is not comprehensive enough and the omissions are glaring. There is nothing specifically on loss of mortgaged property documents by banks, delays in handing over original documents after full repayment of loans, loss or damage of items in bank lockers. There is a mention of double debits at Points of Sale (PoS) but not a squeak on debit at the customer's end but no credit to the merchant necessitating another swipe or cash payment and no time frame for reconciliation and refund from the bank? Unsolicited calls for add-on cards or insurance for cards finds a mention but it is silent on tele-marketing by banks for credit cards and loans. What about charging for sms alerts but not sending them regularly? The **Code of Banks Commitments to Customers** lists more grounds under 10 heads. And there is the **Fair Practices Code**. Why should the

[5] https://indiankanoon.org/doc/5072712/
[6] https://indiankanoon.org/doc/82724656/

grounds in the Ombudsman Scheme read like wheels within wheels? It is designed to empower or confuse customers?

BANK ACCOUNT OPENING BLUES:

The glib talk about 'instant welcome kits' is often restricted to the pre-account opening stage, post which, you may not even get a seat when you visit the bank to follow up on delays.

The Know Your Customer (KYC) documents are routinely and repeatedly sought by banks. Why can't a simple check of self attested documents suffice? When banks nitpick so much, what explains their mounting Non Performing Assets? If banks insist on KYC, why can't customers be given KYB or 'Know Your Bank' in return?

I know of a big private bank delaying the opening of a savings account despite all the documents being in order, encashing the initial deposit cheque and siphoning off the money to a dummy or suspense account! So the account from which the customer issued the cheque is debited but the new account is not credited because it is yet to come into existence! The new account is opened after a few days. The **National Consumer Disputes Redressal Commission in Haryana Packaids vs. Punjab & Sind Bank**[7], upheld the Delhi State Commission's judgment to pay compensation to the customer when a pay order was put into a sundry account.

When banks lend money even for a one or two day period, isn't it possible that the customer's initial deposit is squirreled away by the bank to be lent to others at a hefty rate of interest? The loss of interest for a single customer may be negligible but if it's a regular practice, you can sniff out a scam.

The **Supreme Court in Om Prakash Vs Asst. Engineer, Haryana Agro**[8] held that if a trader intentionally delays the delivery of any goods to the consumer, because of which the consumer suffers, it shall amount to an unfair practice. The remedy need not be limited to compensation. The **National Consumer Disputes Redressal**

[7] https://indiankanoon.org/doc/50756124/
[8] https://indiankanoon.org/doc/1655260/

Commission in Awaaz Punita Society Vs RBI & Others[9] ruled that if there is any unfair trade practice on the part of banks, under Section 14(1)(f) of the Consumer Protection Act, they can be directed to discontinue such practices. In a similar vein, Section 35A (b) of the Banking Regulation Act, empowers the RBI to issue directions to prevent banks from acting in a manner "prejudicial to the interests of depositors."

NET BANKING GLITCHES:

If you've taken a loan from a bank, can you possibly cite a marriage in your family as an excuse for non-payment of your EMI? By the same logic, could, for instance, the merger of five associate banks with State Bank of India, that warranted transfer of data and updation, justify dysfunctional net banking, failed debit card transactions and cashless ATMs? Just like an event in a customer's life is extraneous to repayment of a loan, a business function in a bank should have nothing to do with normal operations. Not quite. Because the customer and a bank are not 'Even Stevens'.

If you default thrice on a vehicle or home loan, the bank will initiate steps to seize your hypothecated car or two-wheeler or move to take over your property under the SARFAESI Act. However, if you are unable to log into your account online, the bank may first play Kumbhakarna and sleep over the grievance for a while, followed by trouble shooting tips for dummies like 'try deleting cookies, cache and browser history'. Banks are custodians of public money. And it's an essential service. Not being able to access your account online for reasons attributable to the bank's internal dynamics, negates the government of India's pet 'Go Cashless' slogan. It is akin to being locked out of your home because the care-taker changed and the keys are yet to be found!

How many of us have read the terms and conditions of internet banking services? I found three clauses in State Bank of India's site lopsided. Clause 4 states that "the Bank at its sole discretion may also make additions/deletions to the Internet Banking Services being offered

[9] https://indiankanoon.org/doc/868342/

without giving any prior notices or reasons." I wonder if this constitutes 'free consent' under Section 14 of the Contract Act. Can consent be a default option? As the customer has no choice and is automatically deemed to agree with these terms, does it constitute 'undue influence' covered by Section 16 of the Contract Act, as the bank is in a position to dominate the will of the customer and uses that position to obtain an unfair advantage over him?

Clause 5 B is sweeping. The customer agrees not to hold the bank responsible or liable for "any loss as a result of compromise of User-id and password by the User himself or if the User has failed to follow the Internet Banking Service instructions." Who will determine compliance by the user and loopholes caused by the bank? Under sub clause D, the bank claims a right to deactivate the internet banking login of any user due to "unsatisfactory behaviour in the account." Who defines this conduct? Would such terms be viewed as an 'unfair trade practice' attracting Section 2(1)(r) of the Consumer Protection Act?

Banks can flood customers with promotional offers, some even managing to bypass the Do Not Disturb registry. But how many customers of merged banks have received information about any change in the rate of interest on loans taken or fixed deposits made or card charges? Do banks take customers for Thanjavur dolls that would nod for everything?

BANKS MISPLACING MORTGAGED PROPERTY DOCUMENTS:

The Public Notice section of newspapers will reveal how common this trend of banks losing original documents of their customers truly is. Not all banks register an FIR and hand over a Non Traceable Certificate to the Customer. Many prefer to just routinely issue a Lost Notice in a newspaper and a certified copy of the documents. And they would underplay their serious lapse by assuring the customer that it would not affect the title or the prospect of getting further loans on the strength of certified copies of title deeds. It jolly well does. RTI applications filed by customers revealed that not all banks accept certified copies of title deeds as security for loans.

That banks are custodians of public money and assets and cannot do a Pontius Pilate by washing their hands off was a message sent out by the **National Consumer Disputes Redressal Commission in C.L. Khanna vs Dena Bank**[10]. The Commission held in 2005 that *"there is clear deficiency on the part of the Bank in not returning the title deeds. The title deeds were given to the Bank in good faith and considering the Bank would be the safest place for keeping such title deeds."*

And the compensation awarded need not be for the actual loss but also for mental agony that is also the result of the need for prolonged follow up with banks. The **Supreme Court** has held in **Ghaziabad Development Authority Vs Balbir Singh**[11] that *"The word compensation is of a very wide connotation. It may constitute actual loss or expected loss and may extend to compensation for physical, mental or even emotional suffering, insult or injury or loss.* Perhaps guided by this principle, the **Uttar Pradesh State Consumer Disputes Redressal Commission** had in a landmark case in 2012, ordered **LIC Housing Finance**[12] to pay a customer 85 lakh rupees for losing his sale deed. This was based on the market value of the house.

When banks can publish photographs of defaulters with captions like 'dishonest borrowers', how about aggrieved customers doing the same with titles like 'negligent lenders'?

DIS-CARDING ANTI CONSUMER PRACTICES:

You present your debit card after a meal at a restaurant or shopping at a mall, enter your PIN and get a text message from the bank confirming the transaction. But the Merchant Establishment at the Point of Sale (POS) claims the transaction failed even if you show him the debit message. You are forced to swipe your card a second time, which may fail again or pay cash. So you may end up making a double payment for the same transaction, with the vendor invariably assuring you that the money debited from your account for the failed

[10] https://indiankanoon.org/doc/888813/
[11] https://indiankanoon.org/doc/1682813/
[12] https://timesofindia.indiatimes.com/city/lucknow/LIC-to-pay-Rs-85-lakh-for-losing-sale-deed/articleshow/16563747.cms

transaction will be refunded by the bank in 48 hours. In reality, it takes at least a week for even verification, let alone refund to happen.

A card transaction may fail for several reasons. An incorrect PIN, an insufficient balance, damaged or expired card can be attributed to the customer. But usually, it's a fault with the POS machine or connectivity at the merchant's end. Or a problem with the payment gateway or the bank's server. In some cases, even a fraud played by the merchant. These scenarios have a distinct anti consumer ring to them. Why can't the banks and merchants have a foolproof system where the actual reason for the failed or declined transaction is printed on the slip?

With the government advocating digital payments, why can't a failed transaction and resultant wrong debit have an immediate 'bounce back' effect? Why does the bank take a few days to a week or even more to reverse the entry? Or sometimes even to throw light on the actual status of a transaction? The **National Consumer Disputes Redressal Commission in State Bank of India Vs Dr.J.C.S Kataky**[13] held that *"once the complaint was made citing specific incidents of unauthorised withdrawal, it was the duty of the Bank to have carried out the necessary verification in the matter, rather than washing their hands off the whole episode."*

In **Dipika Pallikal Vs Axis Bank**[14], it was found that the Complainant's transactions were declined abroad citing 'Insufficient Funds' when the balance was more than ten times the swiped amount! Exemplary compensation was awarded by the **Chennai District South Forum** for mental agony.

The **Compensation Policy (Banking Services) 2016 of SBI**[15], for instance, under Clause 4.1 for erroneous debit, gives the bank 7 working days where no third party is involved to verify the transaction reported. Where third parties are involved, it gives itself a month for verification. Third parties are not from another planet and should be a

[13] https://indiankanoon.org/doc/25533575/
[14] https://timesofindia.indiatimes.com/city/chennai/Chennai-consumer-forum-directs-Axis-Bank-to-pay-Rs-5-lakh-compensation-to-Dipika-Pallikal/articleshow/32590182.cms
[15] https://www.sbi.co.in/portal/web/customer-care/compensation-policy

call or email away. Do banks send communication through pigeons to justify such a long period? Another sub clause states that where neither the bank is at fault nor the customer, but the fault lies elsewhere in the system, the bank will help in restoring the actual amount involved. But restoration can only take place after verification! Why should a consumer's money be locked up for no fault of his? What about the interest on the money for this period? What if a customer has limited funds in his account which are erroneously debited twice at a business establishment and he has to buy medicines urgently or needs the money for an emergency?

The **Haryana State Commission in Dr.Subhash Chander Vs SBI**[16] referred to the Compensation Policy on fraudulent transactions which states that *"the amount will be restored to the affected customer account without delay/demur, once the fraud is established."* But don't the words "with due verification" that follow, negate the "without delay" assurance?

This is where the National Payments Corporation of India (NPCI), an initiative of the Reserve Bank Of India (RBI) and Indian Banks Association (IBA) under the Payment and Settlement Systems Act, 2007, must live up to its lofty goal of 'Customer Centricity'. It strives to "pre-empt our customers' future needs and expectations and bring about innovations in our products and services, in proactive anticipation even before the need has arisen."

Many card conditions are cloaked. Sample some. Bank will approve\reject any card transaction at its discretion. Transactions as per bank records to be conclusive and binding on the cardholder. Verified and corrected amounts are to be binding on the cardholder. The Bank has absolute discretion to change terms and communicate them in any manner. Legal proceedings to be only within the jurisdiction of the bank's headquarters.

WHY CUSTOMERS CANNOT BANK ON LOCKERS:

If you want to safeguard your valuables like property documents, jewellery or certificates, a bank locker is a common preference.

[16] https://indiankanoon.org/doc/86795289/

Exploiting this need, many banks insist on a deposit of twenty five to fifty thousand rupees depending on the size of the locker. Is this legal? The Committee on Procedures and Performance Audit of Public Services had observed that linking the locker facility with placement of fixed or any other deposit is a "restrictive practice" and should be "prohibited". But the Reserve Bank of India seems to have interpreted the words "beyond what is specifically permitted" in the guidelines, to allow banks "to obtain a Fixed Deposit which would cover 3 years rent and the charges for breaking open the locker in case of an eventuality" from new hirers. The deposit amount is calculated at the annual rate of interest it fetches multiplied by three years of locker rent. Such practices may fall under 'anti competitive agreements' covered by Section 3 of the Competition Act as they have the trappings of a 'tie-in arrangement' described in Sub Section (4) (a) of the Statute.

When annual locker rent is collected in advance, what is the need for this deposit? When customers keep their life savings and valuables inside, what is the percentage of hirers who would default on payment of rent and leave their lockers unoperated to warrant banks breaking them open? What explains the banks' presumption of the "eventuality" of non-payment of rent and non-operation of lockers? Are such 'eventualities'more common than bad debts and non performing assets?

NOMINATION FACILITY:

On the one hand, banks take the plea that as they make no inventory of the contents of lockers, they are not responsible for damage or loss suffered by the hirers. But when a locker with no nominee registered needs to be opened by legal heirs, they insist on an Indemnity Bond with a Surety, despite the claimants producing Death Certificates, Legal Heirship Certificates with proof of identity and address and the bank's legal protection under Sections 45 ZC to 45 ZF of the Banking Regulation Act.

After Courts and Consumer fora had ruled that in the case of lockers, the relationship between banks and customers are not the equivalent of a landlord and tenant but that of a bailor and bailee, the

RBI had advised banks to exercise due diligence. The **National Consumer Disputes Redressal Commission in Canara Bank Vs Agnes D'Mello**[17] had referred to Section 73 of the Contract Act while ruling that the bank could not absolve itself of the responsibility to pay damages for the loss of locker contents. Abundant caution need not take on the aggravated form of paranoia. The **Calcutta High Court in Rama Chakravarty Vs Manager, Punjab National Bank**[18] held that *"the Bank is not required to behave like a busybody and develop any headache over the matter but is expected to adopt an attitude of cooperation, and not of a combatant, to its customers or their representatives."*

In the first place, why do banks entertain locker applications without registration of nominees? When they can go on and on about compliance with Know Your Customer (KYC) norms, why can't they insist on nomination? Although they are required to enter the name and registration number of nominees even on savings account passbooks, not all of them do this. This is a violation of Rules 2 (9), 3 (8) and 4 (9) of the Banking Companies Nomination (Rules), 1985. How will people know if they are nominees? A fair banking practice would be to send letters to nominees whenever a nomination is registered.

ARE LOCKERS WATER PROOF?

The 2015 Chennai deluge highlighted the issue of safety of lockers. Many banks are located on the ground floor and were submerged when the water level rose beyond six feet. Even if the lockers of banks are not iron clad, their agreements would be! The Reserve Bank of India policy is that "the bank will, in no way, be responsible/liable for the contents kept in the locker by the hirer. In case of theft, burglary or similar unforeseen events, no action will be initiated as per law." Force Majeure will always be the first defence of the bank if contents are damaged due to natural disasters. But there's a rider. Banks must take all necessary steps to protect the contents in their lockers.

[17] https://indiankanoon.org/doc/1074934/
[18] https://indiankanoon.org/doc/343736/

Banks claim that they share a landlord-tenant relationship with locker holders as they would be unaware of what is kept inside the locker. Moreover, a locker can only be opened by the customer along with the master key held by the bank. As there is an element of trust involved, doesn't it take on the form of bailment, making it a bailor - bailee equation? The **National Consumer Disputes Redressal Commission in Jyoti Satya Vs Bank of Maharashtra**[19] rejected the landlord-tenant argument of the bank in a case of robbery and held that *"valuable articles were left in lockers only on the assurance that the bank would provide complete security."* Lockers must ideally be located on first or higher floors and definitely not on the ground floor. That should form part of the bank's due diligence.

In a case where currency notes and documents in the locker were destroyed by termites, the **National Consumer Disputes Redressal Commission in Bank of India vs Smt Kanak Choudhary**[20], awarded compensation to the customer and reiterated that the bank *"was bound to ensure that the locker remained safe in all respects."*

'CLAUSE' AND EFFECT: UNFAIR TRADE PRACTICES:

In a scathing indictment of lopsided clauses in 'standard form contracts', the Law Commission in its 103rd Report noted that "these are really pretended contracts. They are called contracts of adhesion (from the French term) because, in these, a single will is exclusively predominant, acting as a unilateral will, which dictates its terms to an indeterminate collectivity on a take-it-or-leave-it basis. The qualifications are buried in small print and imposed upon the customer. They are not open to discussion, nor are they subject to negotiation between the parties. The contracts are produced by the printing press. The pen of the individual signing on the dotted line does not really represent his substantial agreement with the terms in it, but creates a fiction that he has agreed to such terms."

[19] https://www.rediff.com/money/2004/aug/14spec1.htm
[20] https://indiankanoon.org/doc/1092326/

These are classic unfair trade practices covered under Section 2(1)(r) of the Consumer Protection Act. The **National Consumer Disputes Redressal Commission in Rohit Bajaj Vs ICICI Bank**[21] held that unilateral contracts *"cannot be termed as intentional contract between the parties, and, in some cases, it may amount to an unfair trade practice."* The next time consumers are asked by banks to sign against an 'x' mark on the dotted line, they must behave like pedestrians at a signal: Stop, read and proceed.

RECOMMENDATIONS:

1. Branch Managers must function as a more effective 'first line' of grievance redressal with targets set on resolution.
2. Relationship Managers must only address problems of customers and not engage in unsolicited commercial communication.
3. Banking Ombudsmen need not be only bank officials but can be drawn from different fields to obviate bias.
4. The Grounds of Complaints under the Banking Ombudsmen Scheme must be more comprehensive to include common grievances without too many sub texts and Codes.
5. The Procedures for filing of complaints before ombudsmen must be simplified. Alternatively, advocates must be allowed to represent complainants.
6. On the lines of KYC, banks must provide customers with KYB (Know Your Bank) details like Non-Performing Assets and clear timelines for various services.
7. Customers must be paid compensation for disruption in net banking services beyond a prescribed time limit and for ATMs that do not dispense cash on any given day.
8. Banking Guidelines, Codes & Contracts must not be lopsided.

[21] https://indiankanoon.org/doc/627843/

9. It must be made mandatory for banks to issue proper and immediate acknowledgement of title deeds before the Memorandum of Deposit of Title Deeds is done at the time of Registration and return the Original Documents within a prescribed time frame on proof of full repayment of loans.

10. If banks are allowed to publish lists of defaulters, RBI must publish lists of negligent lenders when banks original documents of customers. A proper protocol – of giving the customers FIRs, Non Traceable Certificates, Clippings of Public Notices and Indemnity Bonds in cases of loss.

11. Banks must not insist on Fixed Deposits for Lockers. Locker rent may be collected annually in advance. Lockers must be water proof. Every locker holder must have a nominee.

12. Banks must send an intimation to all nominees of accounts, deposits or lockers about their names mentioned with relevant details.

GRIEVANCE REDRESSAL MECHANISM IN BANKING SECTOR

Kumaresh .S*

ABSTRACT:

Grievance Redressal (GR) refers to the process of accepting, addressing and alleviating the complaints of consumers. When a customer of a bank encounters a grievance, he may utilize the Grievance Redressal Mechanism (GRM) made available to him by the respective bank. An effective GRM is necessary in banking sector for receiving and redressing consumer grievances courteously, promptly and satisfactorily. For this purpose, various efforts were made by the Reserve Bank of India (RBI) via directions to banks, both public and private, into creating appropriate GRMs. Due to the directions most banks have a GR policy which they strive to follow in order to resolve any complaint that may arise. GRM can be classified in a two-folded manner: Internal Grievance Redressal Machinery (IGRM) and External Grievance Redressal Machinery (EGRM). The IGRM has several levels of escalation and each level needs to be exhausted (or 30 days must have expired since the date on which the complaint was made) before EGRM can be utilized. EGRM is also known as the Banking Ombudsman (BO), the authority appointed by the RBI to redress grievances which the apex level in the Internal Machinery failed to redress. The BO was effectuated by the Banking Ombudsman Scheme 2006, which enables an expeditious and inexpensive forum to bank customers for resolution of complaints relating to certain services rendered by banks. The scheme specifies the BO's powers and jurisdiction, grounds of complaint, procedure for filing complaints, etc. The purpose of this article is to analyze the various aspects of Grievance Redressal Mechanism in banking sector with reference to the Master Circular on Customer Service in Banks and the Banking Ombudsman Scheme. Further, some cases handled by the BO have been included to show the effectiveness of Office of BO.

* IV year, B.Com LLB (hons.), School of Law, Sastra Deemed-to-be University, Thanjavur.

INTRODUCTION

A consumer grievance is an expression of dissatisfaction on a consumer's behalf to a responsible party. Consumer complaints are part of the business life of any corporate entity. This is more so for service organizations like banks. In the present scenario of competitive banking, excellence in customer service is the most important tool for sustained business growth.

Grievance Redressal (GR) refers to the process of accepting, addressing and alleviating the complaints of consumers. GR is essential for maintaining the goodwill and trust of customers. An effective GR Mechanism (GRM) is necessary for the banking sector for redressing consumer grievances courteously, promptly and satisfactorily. If the complainant's grievance is not redressed, it will only deter him/her from continued availing of services of the corresponding bank. When a customer of a bank encounters a grievance, he should be able to utilize the GRM made available to him by the respective bank.

In the banking sector, grievances may be of several kinds. For example, non-payment or inordinate delay in the payment or collection of cheques, non-adherence to prescribed working hours, levying of charges without adequate prior notice to the customer, etc are some of the grievances which a customer may encounter while availing banking services.

Being the regulator of the banking sector in India, Reserve Bank of India's (RBI) important objective is to ensure that grievances of customers of banks are redressed and that relief is provided to the aggrieved.

This article aims to shed light on the efforts made by the RBI with regards to GRM in banks, procedures to be followed for GR, various levels of GRMs, the Banking Ombudsman Scheme and to finally ascertain the effectiveness of the existing GRM as well as the Consumer Fora as an alternative and to suggest improvements in the GRM that would benefit consumers.

GRIEVANCE REDRESSAL MECHANISM - RBI'S EFFORT

RBI, being the apex banking authority of the country, has a direct interest in the establishment of GRMs for the country. The most critical efforts made by the RBI towards the creation of appropriate GRMs, both internal and external, are visible through their directions in the Master Circular on Customer Service in Banks and the Banking Ombudsman Scheme of 2006. The Master Circular provides for various measures to be taken by banks to redress the grievance of their consumers and also suggests for analysis of complaints - identifying areas from which complaints are frequently received; sources of complaint; systemic deficiencies; and for initiating appropriate action - to make the GRM more effective.

Banks are also advised to place the detailed statement of complaints and its analysis on their website for information of the general public at the end of each financial year.

In addition to the Master Circular, RBI, in its Monetary Policy Statement of 2005, announced setting up of the Banking Codes and Standards Board of India (BCSBI) in order to ensure that a comprehensive code of conduct for fair treatment of customers was evolved and adhered to.

The main objectives of the BCSBI are:

- To plan, evolve, prepare, develop, promote and publish comprehensive Codes and Standards for banks, for providing fair treatment to their customers.

- To function as an independent and autonomous body to monitor, and to ensure that the Codes and Standards adopted by banks are adhered to, in letter and spirit, while delivering services to their customers.

Later, BCSBI, in collaboration with the Indian Banks' Association (IBA), evolved the Code of Bank's Commitment to Customers, which set minimum standards of banking practices for member banks to follow when they are dealing with individual customers. Through these steps, RBI sought to make GRM more effective and expeditious.

Internal Grievance Redressal Mechanism (IGRM)

RBI has directed banks to ensure that a suitable internal mechanism exists for receiving and addressing complaints from its customers with emphasis on resolving such complaints fairly and expeditiously regardless of the source. For this purpose, banks are advised to have a comprehensive customer GR and compensation policy, which shall include:

- Ensuring that complaint registers are kept at prominent places in their branches.
- Having a system of acknowledging complaints.
- Fixing a time frame for resolving complaints received at different levels.
- Prominently displaying at branches, the names and contact details of officials who can be contacted for redressal of complaints and to include the name and other details of the concerned Nodal Officer appointed under the Banking Ombudsman Scheme, 2006.
- Displaying on their websites, the names and other details of officials at their Head Office / Regional Offices / Zonal Offices who can be contacted for redressal of complaints, including the names of the Nodal Officers / Principal Nodal Officers.
- Displaying the names and other details of their CMD / CEO and also Line Functioning Heads for various operations on their websites to enable their customers to approach them in case of need.

- Ensuring that the Principal Nodal Officer appointed under the Banking Ombudsman Scheme is of a sufficiently senior level, not below the rank of a General Manager.

- Displaying the contact details of the Principal Nodal Officer in the portal of the bank so that the aggrieved customer can approach the bank with a sense of satisfaction that she/he has been attended at a senior level.

- Providing wide publicity, through advertisements, about the grievance redressal machinery

- Making GRM simpler even if it is linked to the call centre of customer care unit without making the customers face hassles.

If complaints are not redressed within a month, the concerned branch should forward a copy of the statement of complaints to the concerned Nodal Officer under the Banking Ombudsman Scheme and keep him updated regarding the status of the complaint. This is to enable the Nodal Officer to deal with any reference received from the Banking Ombudsman regarding the complaint more effectively. Further, it is also necessary that the customer is made aware of his rights to approach the concerned Banking Ombudsman, in case he is not satisfied with the bank's response. As such, in the final letter sent to the customer regarding redressal of the complaint, banks should indicate that the complainant can also approach the concerned Banking Ombudsman and provide the required details.

Besides, for the sake of reviewing the GRM and making it more effective, banks are advised to:

- Critically examine the working of the IGRM to see if it has been effective in achieving improvement in customer service in different areas.

- Identify areas in which the number of complaints is large or on the increase and consider constituting special squads to look into

complaints on the spot in branches against which there are frequent complaints.

- Consider shifting the managers/officers of branches having a large number of complaints to other branches/regional offices/ departments at Head Offices, where contacts with the public may be relatively infrequent.

- Consider appointing Public Relations Officers / Liaison Officers for mitigating the complaints of customers expeditiously at larger branches and at branches with a large number of complaints.

- Arrange to include one or two sessions on customer service, public relations etc., in training programmes conducted in their training establishments.

- Examine the grievances/complaints regarding congestions in the banking premises and take action for augmentation of space, whenever necessary.

To further boost the quality of customer service, banks are advised to appoint an Internal Ombudsman (IO). The IO should not have worked in the bank in which he/she is appointed. The IO will be a forum available to bank customers for GR before they can even approach the BO. RBI tightened the selection and operating procedure for IO in banks, making it mandatory for lenders with more than 10 branches to have an independent authority to review complaints that were partially or wholly rejected by the respective banks.

By providing appropriate directions regarding the receipt of complaints, transparency of information about GR, appointment of Nodal Authority, reviewing the IGRM and taking action towards fixing any flaws, RBI has attempted to make the IGRM in banks effective. Further, appointment of IOs is a huge step towards speedy redressal of grievances.

In order to protect the interests of consumers by limiting their liability in case of unauthorized online transactions, the RBI issued a circular in 2017. Accordingly,

a. Zero liability, in case of loss due to negligence by bank or third party breach and if the customer informs the bank within 3 days

b. Limited liability if the loss is due to customer negligence where the customer will be liable only till he reports the unauthorized transaction to the bank; or, third party breach and if the customer informs the bank between 3 - 7 days.

c. Liability based on Bank's board approved policy, if there is a third party breach and the **c**ustomer informs the bank after 7 days. Policy details to be shared at the time of opening of accounts.

External Grievance Redressal Mechanism (EGRM)

Banking Ombudsman

EGRM refers to the GRM outside that of the bank, for when the IGRM fails. One such mechanism is the Banking Ombudsman Scheme of 2006. Banking Ombudsman is a senior official appointed by the RBI in order to redress the grievances of customers when the banks themselves fail to do so.

Consumers always have the option of approaching the Consumer Fora. However, it should be remembered that once the matter is filed and is pending before the Forum, the Office of the BO will not entertain the same.

There are 21 BO offices in India, mainly in different state capitals. The office to be approached depends on the territorial jurisdiction under which the bank is operating. For example, if the source of grievance is in Chennai, then, the aggrieved party can only approach the Office of BO present in Chennai. However, there also exist other conditions for admissibility, which include:

- Complaint to be filed within one year since the failure to redress by IGRM - including time allowed for IGRM, complaint to be filed within 13 months
- If the complaint is found to be frivolous/vexatious
- If the institution which caused the grievance is not covered under BO scheme
- If the complaint is not covered under the scheme (BO scheme provides a list of issues that fall within its purview)
- Complaint once settled by the Office of the BO, cannot be brought up once again before the BO

Clause 9 of the BO Scheme provides the procedure for filing complaints. Though it provides a standard format for lodging complaints, it is not mandatory to follow the same. The complaint may be filed electronically as well.

Complaints can only be made on the grounds mentioned in Clause 8 of the Banking Ombudsman Scheme. These include:

- Non-payment or inordinate delay in the payment or collection of cheques, drafts, bills etc.;
- Non-acceptance, without sufficient cause, of small denomination notes tendered for any purpose, and for charging of commission in respect thereof;
- Non-acceptance, without sufficient cause, of coins tendered and for charging of commission in respect thereof;
- Non-payment or delay in payment of inward remittances.
- Failure to issue or delay in issue of drafts, pay orders or bankers' cheques
- Non-adherence to prescribed working hours;

- Failure to provide or delay in providing a banking facility (other than loans and advances) promised in writing

- Delays, non-credit of proceeds to parties' accounts, non-payment of deposit, etc.

- Complaints from Non-Resident Indians having accounts in India in relation to their remittances from abroad, deposits, etc.

If either party to the dispute does not agree with the Award and wants to pursue the matter further, they can file an appeal before the Appellate Authority. A Deputy Governor of RBI will act as the Appellate Authority. The BO also has powers to reject a complaint during the course of the proceedings, if it has reasons to decide thereof.

Some of the recent cases resolved by Banking Ombudsman are as follows:

- Unauthorised ATM withdrawals:

  The complaint was regarding fraudulent withdrawals amounting to Rs.1,13,000/- from the complainant's account by way of multiple transactions. After receiving a complaint from the customer, the bank was asked to inform whether the complainant had a history of high-value transactions and whether alerts were triggered if the pattern of the transactions were unusual. The complainant had acknowledged that he had received a phishing mail and the bank claimed that he may have divulged personal information in his revert to the mail. However, the Banking Ombudsman was of the view that the bank had failed to adhere to RBI's instructions relating to monitoring of transaction pattern of the usage of card of the complainant and building of a system of call referral. If the bank had done velocity checking and alerted the complainant, the loss could have been avoided had the bank taken measures to block the account. As per BO’s advise, the bank was advised to pay the amount of Rs.1,13,000/- to the complainant.

- Fraudulent Collection of Cheque:

  A complaint was lodged regarding fraudulent encashment of a cheque for Rs.2,36,337/- issued in favour of beneficiary drawn on collecting bank. The complainant stated that he deposited the cheque in collecting bank for collection. It was informed by issuing bank that the said cheque was missing and it already stood cleared in Cheque Truncation System. On further investigation, it was found that the cheque was credited in the account of a third person in some other bank (neither issuing nor collecting). He had further stated that as per police investigation, the cheque was not stolen from issuing bank and also the cheque was not verified under UV scanner. The issuing bank in its reply submitted that the fraud did not occur at their branch. The third bank opened an account of a fraudulent person and made payment in his account. CCTV footage from issuing bank was taken by police. Police did not find any evidence that the cheque was stolen from issuing bank. The third bank was advised to submit original cheque and KYC documents of the account in which cheque was credited, to which, the bank replied that the account of the third person (beneficiary of cheque amount) was opened with due diligence and proper KYC documents were obtained. The third bank was given ten days' time to investigate the matter. It was advised to send the cheque to a forensic lab for investigation and in the meanwhile pay the disputed amount to the complainant. Eventually, the third bank remitted Rs. 2,38,337/- to the complainant.

In both cases, BO made sure that the complainant's grievance is redressed and the bank at fault bears the burden of the same.

BO SCHEME - PROS AND CONS

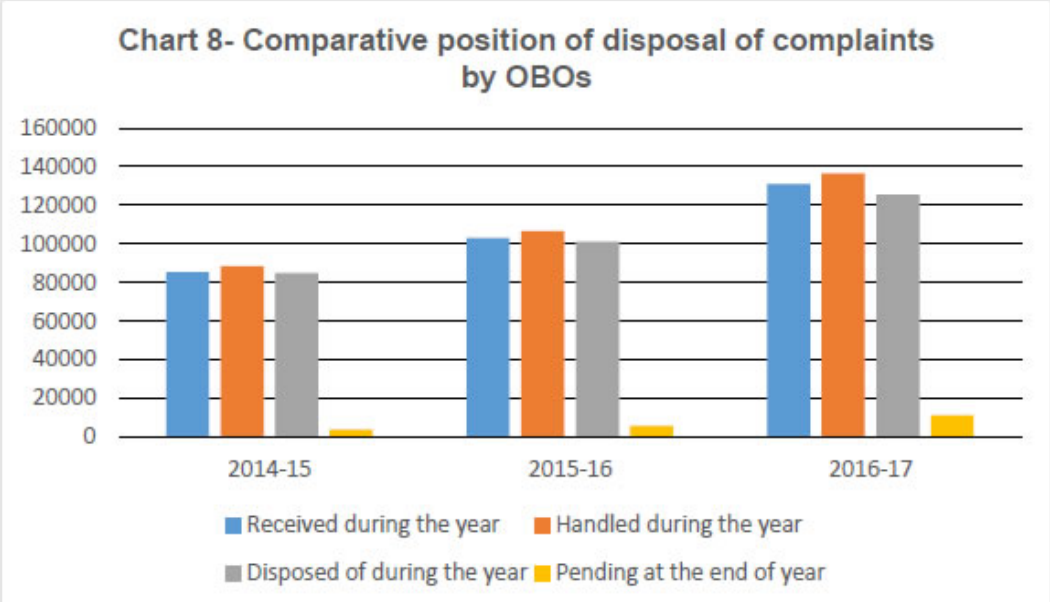
Data points out to the BO Scheme being effective in dealing with customer complaints. During 2016-17, Office of BOs handled 1,36,511 complaints, including 5,524 complaints pertaining to the previous year. As on June 30, 2017, OBOs managed to dispose 92% of the complaints

handled during the year. Table 9 and Chart 8 of 2016-17's Annual Report of BO Scheme, shown below, indicates a comparative position of disposal of complaints by Office of BOs.

Table 9 - Comparative position of disposal of complaints by BOs

Number of complaints	Year		
	2014-15	2015-16	2016-17
Received during the year	85131	102894	130987
Brought forward from previous year	3307	3778	5524
Handled during the year	88438	106672	136511
Disposed of during the year	84660	101148	125319
Rate of Disposal (%)	96%	95%	92%
Carried forward to the next year	3778	5524	11192

Source : RBI, Table 9 of Annual Report of BO Scheme, 2016-2017



Source : RBI, Chart 8 of Annual Report of BO Scheme, 2016-2017

Although the rate of disposal declined from 95% to 92% during the year, the actual number of complaints handled increased by 28%. Compared to previous years, complaints increased by 11% in 2014-15, 21% in 2015-16 and 27 % in the year 2016-17.

Advantages of the BO Scheme includes the following :

- It helps with the speedy delivery of justice by being an alternate source of GR specialized in the subject matter concerned.
- It is framed in such a manner that it does not oust the jurisdiction of other courts. This allows aggrieved parties to not hesitate in using the BO as a primary forum for resolution of disputes regarding banks.
- BO is in position to do justice on a case-by-case basis. BO is not bound by the precedents and can, in certain circumstances, ignore technicalities and legal rules of evidence while resolving disputes.
- BO's offices have also started outreach activities for creating awareness among customers like interface with banks, organizing awareness camps, participation in exhibitions, responding to readers' queries, etc.

At the same time, there are also certain disadvantages in the current scenario :

- Though supposed to be an external, independent entity, Office of BO is not easily approachable - one of the reasons being that it is housed within RBI.
- In some instances, impolite behaviour and delay in responding to customers have been common causes of distress.
- Consumers feel that rulings are, at times, predetermined.

- There is still a need for increased consumer awareness regarding the BO scheme, especially in semi-urban and rural areas, where the percentage of total complaints received is comparatively less, indicating ignorance of the scheme.

- Banking Ombudsman is limited to the grounds on which a customer can file a complaint against a bank and there is a dire need to expand the scope of ombudsman in the changing IT environment.

CONSUMER FORUM

Banking services come under the umbrella term "services" defined in Section 2(1)(o) of the Consumer Protection Act, 1986. An aggrieved consumer of a bank may approach the Consumer Fora for redressal of his grievances and seek compensation for mental agony/ harassment. Redressal is provided through a three-tier quasi-judicial system, each of which has its own jurisdictional restrictions. Any person who fulfils the criteria mentioned in the Consumer Protection Act, 1986 may approach the appropriate Fora established in Chapter 3 of the Act.

Some of the grounds of complaints include:

- Refusing or holding back the amount that was due on fixed deposit after maturity.

- Delay in the payment of the amount on term deposits after maturity.

- Dishonour of cheques due to mistake or negligence of the bank.

- Dishonouring of demand drafts because of omission by bank officials.

- Refusing grant of loans without any bonafide reason.

- Causing undue delay in discharging installments of the loan.

Some of the cases handled by the Consumer Fora are :

- **Allahabad Bank vs. Ravindra Flour Mills Pvt. Ltd. - I (2007) CPJ 60 (NC)**

  Facts

  Complainant obtained cash credit limit of Rs.60 lakhs from Petitioner Bank. Complainant repaid the due amount in the account and asked the Petitioner to issue 'No Dues Certificate'. The Petitioner Bank charged Rs.19,713/- towards Penal interest @ 2% from the complainant. Complainant filed a complaint seeking refund of penal interest charged. The District Forum allowed the complaint. The appeal of Petitioner Bank was dismissed by the State Commission. Against this dismissal order, Petitioner Bank filed Revision Petition before the National Commission.

  Issues

  Whether Bank is liable for deficiency in service for charging penal interest @2 per cent on the basis of instructions contained in a Circular issued by RBI?

  Held

  The National Commission rejected the contention of the petitioner bank whereby it contended that the penal interest was charged on the basis of an instruction contained in a Circular issued by RBI, and held that neither was a copy of the said circular shared with the respondent nor was a notice sent to the respondents drawing their attention to the circular. In absence of supplying a copy of said circular or drawing attention of respondents through notice/letter thereto the Petitioner Bank was not legally entitled to charge penal interest at the said rate from the Respondent.

- **Col. D.S.Sachar (Retd.) vs. Punjab & Sind Bank - II (2005) CPJ 130(NC)**

  Facts

  The complainant was having a current account with respondent Bank. The complainant, along with his wife, visited the branch to deposit Rs.45,000/- in the said account. At about 1.45 p.m. when the complainant was at the counter, someone snatched the money from his hand and despite raising a loud alarm and chasing, the snatcher fled away on a scooter standing outside the premises of bank with the engine on. Complainant filed the complaint before the District Forum alleging deficiency in service on the part of Respondent Bank as at the time of the incident, there was no security guard/gunman present at the entry/exit gate of the Bank. Collapsible doors of the main gate were not chained and the bank was under a duty to sound the siren alarm. The District Forum dismissed the complaint. On appeal, the State Commission also dismissed the appeal. Against dismissal order of the State Commission, Complainant filed Revision Petition before the National Commission.

  Issues

  Whether liability for payment of money can be legally fastened on respondent Bank, on the ground of it being deficient in service under section 2(1) (o) of Consumer Protection Act, 1986?

  Held

  Ensuring safety of the money to be deposited and/or withdrawn inside the bank premises is an implicit part of service rendered by a bank to its consumer. The Respondent Bank being deficient in service cannot escape liability for payment of said money by way of compensation to the petitioner, with interest.

SUGGESTIONS AND CONCLUSION

In order to improve the GRM, the following steps shall be considered:

- More Offices of BO may be established to address the increase in complaints and make them more approachable for consumers from districts.

- With regard to complaints in IGRM, automation can be used as a way to address basic issues which can be solved without human intervention. This would allow for focus to be on more complicated issues.

- More effort should be put towards consumer awareness. The number of complaints from rural/semi-urban places is low compared to those from urban areas and metros.

- Complaints should be analyzed regularly and identifying/ removing the root cause should be prioritized.

- Expand the scope of Ombudsman due to various changes in the past decade, especially with regards to IT. That is, grounds of complaints should be increased so as to accommodate more complicated issues which arise with technological advances.

- Banks should be easily approachable and address issues as soon as they surface, to avoid similar complaints from taking place.

- Customer care and the escalation levels should be user friendly with appropriate email ids for consumers to register their complaints.

- Incentives could be given for banks with the least amount of complaints and the highest customer satisfaction in order to further motivate banks to take corrective actions towards issues that may lead to complaints.

To quote Mahatma Gandhi, *"A customer is the most important visitor on our premises. He is not dependent on us. We are dependent on him. He is not an interruption of our work. He is the purpose of it. He is*

not an outsider of our business. He is part of it. We are not doing him a favour by serving him. He is doing us a favour by giving us the opportunity to do so."

Since consumers are vital to any organization, including banks, every effort must be taken to satisfy them. An effective GRM is useful for addressing any dissatisfactions that the consumers might have. With appropriate GRM, consumers are encouraged to avail services as there is a promise of speedy and effective redressal.

Thus, it is important for banks to recognize their duty towards consumers and act accordingly so that they earn their trust and goodwill.

LIST OF REFERENCES

1. Master Circular on Customer Service in Banks.
2. Circular on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions.
3. Banking Ombudsman Scheme, 2006.
4. Code of Bank's Commitment to Customers.
5. Annual Report on Banking Ombudsman Scheme, 2016-17.
6. Consumer Protection Act, 1986.
7. www.consumereducation.in/monograms/caselaw_banking.pdf.

PRIVACY ISSUES IN BANKING TRANSACTIONS – A COMPARATIVE ANALYSIS

U Shraddha Bhatt*
&
Sreedevi Anand Nadig

ABSTRACT

Technology, today is a fast-growing sphere. It can be said that technological innovations are increasing in number at a rapid rate. Banking operations and transactions are being digitized today as India moves towards a "cash-less" economy.

But, are the laws of India adequate enough to protect the rights of the people prior to and after entering into such transactions, largely their privacy? Are laws such as Information Technology Act, 2000, Banking Regulation Act, 1949, RBI guidelines etc., foolproof and efficient enough to regulate these digital transactions carried out by banks and do they hold the power to make banks accountable for defaults or violation of any rights or duties?

Other countries and jurisdictions have stronger laws which exclusively regulate and govern digital transactions. The United States, for example follows sectoral legislation and is known to have sturdier confidentiality laws regarding banking transactions via digital means. In India, however, the laws regarding technological advancement are not well developed in comparison.

This paper shall revolve around the loopholes in Indian legislations regarding those laws protecting privacy of customers with respect to banking transactions, especially digital transactions through banks. The paper will also focus on the comparison between Indian laws and foreign legislations in the same sphere. The paper shall also attempt at suggesting required changes to the Indian laws to reinforce them and

* School of Law, Christ (Deemed to Be University), Bangalore, Karnataka.

focus primarily on protection of privacy of those who enter into digital transactions with banks. The paper will attempt to conclude with solutions to the problems discussed and provide suggestions for improvising the status of laws in India with respect to privacy in banking transactions.

INTRODUCTION

"With new technologies promising endless conveniences also come new vulnerabilities in terms of privacy and security, and nobody is immune."

Clara Shih

The above quote was made by the CEO of Hearsay Social, one of the leading digital marketing platforms for financial services, which is of extreme relevance in today's technologically advanced day and age. This quote can be understood in light of the current status of digital privacy online.

The development of a nation depends on various factors and technological advancement plays a vital role in it. In today's day and age, technology is only growing with time and at a very rapid rate. Keeping up with this growth seems difficult and impossible, which is why users tend to go back to traditional methods of practice. For example, banking transactions today can be done from a single device without any hassle, but people who are not aware of computer practice, find it difficult to do so and instead go back to the traditional methods.

Internet is now accessible to all at any corner of the world and this means that any or all data that is uploaded onto the internet can be accessed too. This poses a threat to the privacy of the data that is recorded. The issue of privacy with respect to online data becomes much more serious when it comes to banking transactions or financial services, as it consists of sensitive private information about the customer of such a banking service. The most important part in ensuring security during banking transactions is keeping the pin number and password as a secret, but this too is sometimes hackable, if the bank does not have strong security gears to protect its electronic content.

Online Privacy can be seen as one of the national security threats of the new and improved technological era. The legal system is also evolving at par with technological advancements. The GDPR (General Data Protection Regulation) is the best example in the most recently passed legislation which governs the digital media and its content.

ONLINE PRIVACY AND BANKING

Internet banking has become popular because of its convenience. However, there are still areas of concern such as security and the assurance that the channels of information are secure[1]. Online banking has grown rapidly using today's computer technology thereby providing a new dimension to banking transactions by allowing customers to conduct financial transactions over the Internet. Online banking enables a customer to perform all routine transactions, such as account transfers, balance enquiries, bill payments and credit card applications. Account information can be accessed anytime, day or night and from anywhere.[2] But online privacy issues have generated numerous problems and controversies, some of which are new and some of which are an extension of offline privacy issues. No matter what technology is employed, privacy is always a discussion about the rights and interests of human beings.[3]

A transaction is a business transaction when the two parties involved in this enact the role of a banker-customer. The customer of a bank is one who avails the service of banking or any other financial service. The performance of this task is governed by certain rights and duties. As the banker is the one performing the transaction on behalf of the customer, he holds more responsibility or liability.

The legal framework for banking in India is provided through various statutes such as Banking Regulation Act,1949, Reserve Bank of India Act, 1934; Foreign Exchange Management Act, 1999; Information Technology Act, 2000; Payment Settlement Systems Act, 2007 etc. Banks are under the obligation or duty to provide proper service to the

[1] Manivannan Senthil Velmurugan, An Empirical Analysis of Consumer Protection toward Online Banking Services in the Malaysian Banking Sector: A Biometric Approach, issue 3, J.I.B.L.R. 111- 131 (2012).

[2] M.L Meuter, A.L Ostrom, R.I Roundtree and M.J Bitner, "Self-service technologies: Understanding customer satisfaction with technology-based service encounters" (2000) Journal of Marketing, Pg.64.

[3] Robert Gellman & Pam Dixon, Online Privacy- Contemporary World Issues 31 (ABC-CLIO, 2011).

customer and providing irregular service amounts to deficiency of services under the Consumer Protection Act, 1980. It was held in *Vimal Chandra Grover v BOI*[4], that banking is a business transaction performed between the bank and its customers. Customers are consumers within the meaning of Section 2 (1) (d) of Consumer Protection Act. This obligation extends to e-banking or electronic banking as well.

'Customer Due diligence' commonly known as the 'know your customer' (KYC) is now a widely accepted obligation of banks. Financial institutions are required by law to undertake customer due diligence when undertaking any kind of business relations with them, for carrying out any transactions, especially when there is a suspicion of money laundering or terrorist financing or when there are doubts about previously obtained customer identification data. The process of customer due diligence is conducted to process the consumer's identity and to verify his identification and other relevant documents prior to entering into business with such customer.

Vital to the banker- customer relationship is contract. Once the bank and the customer enter into a business relation and perform any such transactions, the banker has a duty to maintain secrecy or confidentiality about such transactions, until and unless in exceptional cases or when prescribed by law. But, as acknowledged in *Folley v. Hil*[5], the duty of confidentiality is certainly not confined to account holders. Nor is bank liability for faulty advice or breach of a fiduciary or other duty. Having an account with the bank indicates a contractual relationship, which can obviously find remedies, but so too can the myriad of contacts which banks make with customers. It is the trite point but worth making, that banks can enter these many other contracts with customers who don't have an account with them[6].

In the case of *Shankar Lal v SBI*[7], it was observed that one of the duties which a banker has towards his customer is the duty of secrecy, which is a legal duty arising from contract between banker and its

[4] AIR 2000 SC 2181
[5] (1848) 2 HLC 28
[6] Ross Cranston et al., Principles of Banking Law 190 (3rd ed, Oxford University Press, 2017) (1997).
[7] (1987) Cal High Court.

customer. Breach of this duty gives a claim for nominal damages or for substantial damages or injury if resulted from such disclosure. It is not an absolute duty but a qualified one, but is subject to certain reasonable and not essential exceptions, such as – the duty to obey an order under the Banker's Books Evidence Act, a case where a higher duty than private duty is involved such as a threat to national security etc. Apart from these, the banker cannot breach his duty of confidentiality at any time during the banker-customer relationship.

The decision of *Tornier v. National Provisional and Union Bank of England*[8], was that the English law firmly placed an obligation of confidentiality, the legal basis of the duty of bank confidentiality onto banks. It was stated that it was a legal obligation of the banks and not a moral one. If, however, there is breach of duty of confidentiality, then the banker-customer relation could either be terminated, or the customer can claim damages for the breach of such confidentiality. But more than the duty of maintaining secrecy, it can be said that, it is the keeping of trust (or a fiduciary duty). The customer has entered into a transaction and has enclosed all his data to the banker with the belief that the banker is only helping him and this in turn creates trust in the relationship or a fiduciary relationship with him. When it comes to online banking, the customer's sensitive personal information has been recorded in software or an electronic data base and this medium can easily be accessed by anyone and hence it becomes vital to stress on the duty of confidentiality in such a case.

Trust in the electronic medium is known as e-trust, which is believed to increase online customer loyalty. Reducing the human element in banking may have an impact upon customer satisfaction and impede the development of long-lasting relationship with customers.[9]

Electronic signatures are a key component of online transactions with banks. An electronic signature functions in a way comparable to a hand-written signature. An e-signature is a sophisticated way to protect both the bank and the customer. More specifically, the e-signature has

[8] [1924] 1 KB 461

[9] Manivannan Senthil Velmurugan, An Empirical Analysis of Consumer Protection toward Online Banking Services in the Malaysian Banking Sector: A Biometric Approach, issue 3, J.I.B.L.R. 111- 131 (2012).

three key functions: (i) it authenticates the creator of the digital information (ii) it records the creator's intent (e.g.: an agreement with terms) and (iii) it helps ensure that digital content is not tampered with following its creation (i.e. it ensures information integrity)[10]

Customer satisfaction in online banking is based on the ability to conduct secure transactions. The mechanism of encryption, digital authentication, protection and verification in on-line banking that influenced customer's satisfactions on information security increase the consumer's confidence and trust[11].

The factors that affect online banking the most are its accessibility and usability. If the customer is unable to access the information of financial service easily, then it only complicates the process further, which eventually ends up in him adopting the good old traditional methods. Along with accessibility, the information quality of such banking websites plays a major role in creating an impression in the customer's eyes about the bank and its services. The banks along with ensuring that the customer's data and privacy is protected must also warrant that their practices of promoting e-banking also evolve. Only then, the nation can make a move towards a paperless economy and also have a strong technological foundation.

COMPARATIVE ANALYSIS

Personal information in the online world flows routinely without respect to national borders, making online privacy an international issue of some complexity. While some countries successfully impose restrictions - sometimes called censorship- that limit or prevent the flow of other information on the internet and through other means of digital communications, a great deal of data nevertheless flows freely. Individuals, businesses, governments and others can send, receive, and use personal information regardless of their location in the physical world.[12]

[10] Mai Thi Minh Hang, Electronic Signatures in Vietnam: An Online Banking Opportunity, 30. J.I.B.L.R. 627, 627 (2015).
[11] A. Haque, A.Z.H Ismail and A.H Daraz, "Issues of E-banking transactions on Empirical investigation on Malaysian Customers perception ", (2009), 9(10), Journal of Applied Sciences.
[12] Robert Gellman & Pam Dixon, Online Privacy- Contemporary World Issues 73 (ABC-CLIO, 2011).

In 1990, the United Nations adopted Guidelines for the Regulation of Computerized Personal Files. The non-binding guidelines leave it to each state to adopt its own procedures. The UN document, which has not had a major influence in international discussions, also addresses both privacy and transborder data flows. The UN document was the first international data protection standards that included a requirement for an independent supervisory authority. [13]

The Data Protection Directive included one of the first attempts to control data exports in the interest of privacy protection. Articles 25 and 26 establish rules for the transfer of personal data to third countries. The general standard allows data exports to third countries that ensures an adequate level of protection. The directive calls for the assessment of adequacy in light of all the circumstances surrounding a data transfer, including the nature of the data, the purpose of the transfer, and the rules of law, both general and sectoral, in the third country. In order to meet this controversial and much contested EU standard, some nations drafted their privacy laws following the European model. National privacy laws found to meet the EU standard includes Canada, Switzerland, Argentina, and the Isle of Man. Data exports from EU member states to these countries can continue without additional scrutiny or procedure for privacy. The United States, which lacks any comprehensive privacy protections, does not meet the EU standards for adequacy, although it is conceivable that specific sectoral legislation could be found to be adequate.[14]

Currently, there are no universal privacy laws that apply throughout the world. Although some cooperative agreement exists between some countries, each nation typically creates its own approach to privacy regulation, including some countries that have chosen to have no privacy laws at all. That being said, most industrialized countries have enacted at least some privacy protections.[15]

Privacy protection falls into two main categories; sector privacy laws and omnibus privacy laws. The United States uses sectoral regulation while the European Union (EU) uses omnibus regulation. The

[13] Ibid75.
[14] Ibid 83 - 84.
[15] Supra 12.

EU privacy approach has significantly influenced the laws in many countries. [16]

The approach of the United States to privacy differs from that taken by much of the rest of the world. There are no general privacy standards in United States. Instead, the American approach to privacy is defined as sectoral approach. This essentially means that the laws and regulations aimed at protecting privacy apply to particular classes of information or particular record keepers. As a result, in the U.S sectoral approach, the same personal information in the hands of two different American record keepers may be subject to different privacy rules. State privacy laws generally work the same way. The interplay of U.S state and federal law is complex. Some federal privacy laws preempt state to pass similar laws, while other federal laws establish minimum levels of privacy protection that states may exceed. California has been the most aggressive state for enacting privacy legislation, with one famous example of high impact legislation being California's "data breach notification" law. This law influenced other states to pass similar laws. Now, most states have security breach notification laws that require notice to data subject when personal information is inadvertently disclosed. In other areas of privacy, state laws are more occasional and more variable.[17]

Most industrialized countries rely on an *omnibus approach* to privacy legislations. Omnibus privacy laws establish common standards that apply to most public and private activities that involve processing of personal information. Although there are some limited exceptions, omnibus privacy rule generally applies to all record keepers of personal information. More than 50 countries have adopted some form of National Data Protection Legislation of this type. The EU Data Protection of Individual with regard to the processing of personal data and on the free movement of such data. The EU Data Protection Directive requires member states to enact national laws that provide minimum privacy standards[18].

[16] Supra 12.
[17] Ibid 74.
[18] Ibid 75.

India presently does not have any express legislation governing data protection or privacy specially dedicated to the banking sector. The Information Technology Act of 2000 is the only statute that governs and regulates all electronic communications, events, transactions, content and social media. The Act provides for various provisions which give legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication (e-commerce), which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents. Under Section 43, Clause (A)[19], a body corporate who is possessing, dealing or handling any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages to the person so affected. Section 72, Clause (A)[20] is a penal provision and states, disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of the lawful contract is punishable with imprisonment for a term extending to three years and fine extending to Rs. 5,00,000/- The RBI had issued a new circular with respect to internet banking. RBI as a supervisor governs all risks associated with e-banking in a banking transaction. It is also a statutory duty of every bank to keep a customer acceptance policy. This policy must encompass certain aspects of the banker-customer relationship. No account should be opened with a benami or fictitious name. Everything about the customer, including documents of identification should be recorded and verified by the bank, before transacting with their customers as this would put other customer's sensitive information at risk. The recent Supreme Court Judgement in the case of *Puttaswamy v Union of India*[21], has unanimously enforced the right to privacy as a fundamental right under Article 21 of the Constitution of India, which makes it very necessary for India to take a step forward and enact various sectoral privacy laws instead of relying upon one single legislation such as the Information Technology Act, 2000 to take care of every issue faced by parties while doing a e- transaction or a digital transaction of any sort. When it

[19] Information Technology Act, 2000
[20] Ibid.
[21] (2017) 10 SCC 1.

comes to banking specifically, it becomes very necessary to have a specific legislation, because people's financial security is at stake along with that of their privacy, which is now a fundamental right guaranteed to its citizens by the Constitution of India.

CONCLUSION & SUGGESTIONS

Privacy and Security are considered to be the two most important factors prompting user acceptance of online banking services and there is a need for a privacy and security policy to protect consumer's personal and financial information. The success of online banking extensively depends on providing security and privacy for its consumers' sensitive personal data. Security has a significant relationship with consumer protection in online banking services. The reason why the public uses internet banking services is because they feel safe in their online banking transactions and feel secure to provide confidential information. As a fiduciary of the customer, a banker has to bear all this in mind. Hence, when these banking companies or bankers fail in performing their duty of confidentiality or of protecting the customer's sensitive personal data, they are committing a breach of trust. Banking companies should develop necessary control mechanisms against the security issues in order to increase the consumer's usage of online banking services.

The customers must ensure that they do not disclose their financial information such as username, password, and pin numbers etc. to any unauthorised person disguised as the bank. They should change their password on a regular basis so that it is not easily hacked. The security of personal computers is very important for safe internet banking and hence, the customer should be aware of false or hoax news and should not believe such information.

The banks on the other hand must educate its employees regarding cyber law and cyber-crimes and should make sure that they are aware of the various technological technologies and threats and how to keep them in control. Although a banking job is primarily a finance job, it now is coupled with technology and should hence be practiced the same way. The banks must adopt further security measures such

as biometrics. As compared to passwords, biometric accessibility is difficult to gather.

The technological means available today can be used as a boon and to our advantage if they are utilized in a correct manner and for this the involvement of the government plays a major role. The Government should play an active role in increasing the computer literacy rate among people in order to create an IT-savvy society. Any nation can become technologically advanced with the right resources and knowledge but also with the right kind of control measures (which acts as an anti- virus) to keep everything clear of security risks to a large extent.

e-BANKING: SECURITY AND PRIVACY REGULATORY ENVIRONMENT

R. Aswin*

&

R.S. Bharathi**

ABSTRACT:

The internet has played an important role in evolution of banking, influencing how banks interact with its customers and how banks do their business in current era. With the development of internet, electronic banking has emerged, allowing the bankers to do business more effectively, interact with their customers and other corporations inside and outside their industries. After demonetization, a significant change has been observed in the way the banking and financial organizations oversee transactions and offer product and services to their customers. The threats that face electronic banking are concerns of security and privacy of information. It is apparent that concern for *'security and privacy'* is the major barricade in the adoption of electronic banking services. The Information Technology and the networks of the banking sectors have been facing security threats from a wide range of sources including computer-assisted fraud, espionage, sabotage, vandalism etc. Economic development of a country is largely determined by banking and financial system. So, there is a need to study the security and privacy issues in depth from customer's perspective. Along with the study of online portals, the opinion of users will help bankers to understand customer's concern for security and privacy while using electronic banking services. Hence, this work studies the security and privacy issues in electronic banking and suggests theoretical and practical regulatory recommendations to address the issues in electronic banking.

* B.E., B.L. (Hons)., LLM., The Tamilnadu Dr.Ambedkar Law University, Faculty of Law, Government Law College, Dharmapuri.

** B.A., B.L., LLM., The Tamilnadu Dr.Ambedkar Law University, Faculty of Law, Government Law College, Dharmapuri.

INTRODUCTION:

The Internet has played a key role in changing the business today. Electronic banking is a new industry which allows people to interact with their banking accounts via Internet from virtually anywhere in the world[1]. The e-banking system addresses several emerging trends: customers' demand for anytime, anywhere service, product time-to-market imperatives and increasingly complex back-office integration challenges. A secure end-to-end transaction requires a secure protocol to communicate over entrusted public channels and a trusted private channel at both endpoints.

Deployment of secure protocols is necessary because availability of the trusted channels does not exist in most of the environment, especially when banks are dealing with the outside consumers[2]. **A Bank Should Be Something One Can "Bank" Upon[3]**, inspired by the real meaning behind *banking upon something*, a statement of credibility, of confidence, of trust – something that ideally a bank must earn over time by making prudent choices. The solutions to the security issues require the use of software-based systems or hardware-based systems or a hybrid of the two. These software-based solutions involve the use of encryption algorithms, private and public keys, and digital signatures to form software packets known as Secure Electronic Transaction used by Master card and Pretty Good Privacy. Consequently, many businesses are reaching out to customers worldwide using the Internet as its communication channel[4]. This new electronic media of interaction has grown to be known as the *electronic commerce*. "Electronic Commerce integrates communications, data management, and security services, to allow business applications within different organizations to automatically interchange information." In the light of above, the present study discusses the overview of security and privacy risks in e-banking services and discusses the regulatory environment concerning security and privacy of e-banking.

---

[1] "New trends in Banking", M L TANNAN, Banking Law & Practice in India, 27th Edition, Volume 1, Page 229.

[2] Journal of Internet Banking and Commerce

[3] A Bank Should Be Something One Can "Bank" Upon (Dr. Viral V Acharya, Deputy Governor - April 28, 2017 - FICCI FLO Mumbai)

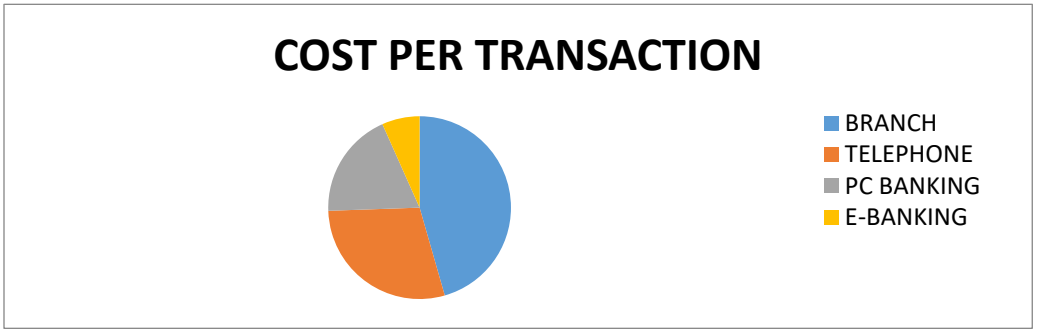
[4] www.academia.edu/.../AN_ANALYSIS_OF_SECURITY_ISSUES_IN_E-BANKING

PARADIGM SHIFT FROM TRADITIONAL BANKING TO E-BANKING:

The Internet is growing at an exponential rate. The number of internet users worldwide would have crossed 3.58 billion in 2017, according to figures from e-Marketer[5], increasing 6.2% next year to reach 42.4% of the entire world's population. This year, the internet will reach more than two in five people in the world for the first time as online audience hits 3.8 billion users globally. As the Internet continues to expand, the convenience associated with electronic banking will attract more customers. In today's market, according to preliminary data from the latest Federal Reserve survey of patterns of consumer spending, almost four-fifths of consumer expenditures are handled by cheques, directly or indirectly.

Moreover, for consumers, electronic money (electronic cash and electronic cheques) means greater efficiency than using coins, paper bills, and traditional banks. The electronic banking system brings the convenience of 24-hour, seven days a week, banking by offering home PCs tied directly to a bank's computers. In addition, electronic money also offers greater security than a paper-and-coin system. Users are able to make a backup copy of their funds and if the electronic money is stolen, the users can invalidate the serial number just as they now stop payment on a paper cheque.

A cost comparison study done by IBM global services consulting group clearly shows the advantage of using Internet as medium for banking services over other traditional mediums (fig.1)



[5] https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

As per the recent survey, traditional banks spend 60%of the revenue generated to run a branch. Whereas, the cost of providing same services via Internet comes out to be only 15%. This is a huge savings for banks and consumer[6].

SECURITY AND PRIVACY ISSUES IN e-BANKING SERVICES

The trend of growth of e-Banking brings many security issues and increasing cost of implementing higher security system for both e-banking users and the banks. The most critical issue of e-banking security is to protect valuable information that is susceptible to unauthorized access by attackers. Various kinds of security threats and issue areas are associated with e-banking system, e.g. communication risks, client authentications, and human factors. In fact, the attacker can choose to hack the current e-banking systems, e.g. trojan horse, botnets, social phishing and so on. The profit driven attacks activity has risen dramatically at every possible level. The Internet related crimes and the security issues were not only applicable for e-banking but also for all server-client Internet applications. Jagticel has discussed how attackers are using "social phishing" to get uneducated victims financial or personal information.

Banking system intrusion shows the vulnerabilities that exists in financial institution, that have been used by those illegal and unauthorized individuals or groups to intrude an area with secure environment. The violation of system security is all about the money, challenges to intercept data, challenges with acquaintance, data breach, and poor authentication and authorization. Financial industry such as banks play a major role in preparing the people with good service, good system, and the best security systems that can meet customer's expectation. It also attracts prospective customers to use trust and using their system to keep their personal data, information and most importantly their money safe. Although there are always vulnerabilities occur around the time, banking system should have a backup plan or other shields in order to handle any malicious behavior, that intend to violate the customer's information. Ways of prevention should be taken

[6] indianresearchjournals.com/pdf/apjmmr/2012/december/2.

care of like the one that has being stated in this paperwork. In order to provide effective and secured banking transactions, there are four technology issues needed to be resolved[7].

The security issue along with the possible attacks may occur due to the insufficient protections. The examples of potential hazards of the electronic banking system are during on-line transactions, transferring funds, and minting electric currency, etc.

The Commercial Banks in India have been facing lot of problems due to Online Banking Crimes. Some of them are enumerated below[8].

- **Unauthorized Access to Computer System or Networking:** This activity is commonly known as hacking.
- **Stealing Information Contained in Electronic Form:** This includes stealing information that is stored in computer hard disks, Removable Storage media, etc.
- **E-mail Bombing:** E-mail bombing refers to sending a large amount of e-mails to the victim, which results in crashing of a person's e-mail account or mail servers, Thereby causing the transaction to fail.
- **Data Diddling:** This kind of an attack involves altering the raw data just before it is processed by a computer and then changing it back after the Processing is complete. This involves flooding computer resources with more requests than it can handle[9].
- **Virus/Worm:** Viruses are the programs that attach themselves to a computer or a file and then circulate themselves to other files and to other Computer on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses, don't need the host to attach themselves to.
- **Salami Attacks:** The key factor here is to make the alteration which is so insignificant that will go completely unnoticed is a single case; for example, a bank employee inserts a program into bank's server which deducts a small amount from the account of every customer.

[7] www.bvicam.ac.in/news/INDIACom%202009%20Proceedings/pdfs/papers/80.

[8] https://www.academia.edu/.../Electronic_banking_impact_risk_and_security_issues

[9] https://www.quora.com/What-is-data-diddling

- **Physically Damaging a Computer System:** This crime is committed by physically damaging a computer or its peripherals.
- **Credit Card Fraud:** The credit card fraud usually affects the merchants. When the Customer uses his credit card for buying things through online shopping and the money deducted from their account does not reach the merchant for his product. It is stolen by the virtual criminal. If the customer has the proof of his order and when he does not receive it, the merchant usually reimburses him on order to maintain his trust in the business[10].

I. Common security problems[11]:

- Denial of service attack
- Distributed denial of service
- Ransom ware
- Malware
- Phishing
- Spear phishing
- Whaling
- Vishing
- Drive-by downloads
- Browser Gateway frauds
- Ghost administrator exploit

The examples of the private information relating to the banking industry are: the amount of the transaction, the date and time of the transaction, and the name of the merchant where the transaction is taking place[12]. Banking is one of the most at risk sectors for privacy violations due to the sensitive and highly personal nature of information that is exchanged, recorded, and retained[13]. Individuals must trust banks with personal identifying information, their financial records, the access information to their accounts, and their credit history[14]. Thus, privacy violations are not taken lightly and heavily impact the individual

[10] https://security.stackexchange.com/questions/76070/what-is-a-salami-attack

[11] https://www.quora.com/

[12] www.academia.edu/.../AN_ANALYSIS_OF_SECURITY_ISSUES_IN_E-BANKING

[13] the IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, July 2012 ISSN (Online): 1694-0814 www.IJCSI.org 440 Copyright (c) 2012

[14] www.iibf.org.in/documents/reseach-report/Tejinder

whose privacy was violated. ***Ways in which a violation of privacy can take place in the banking sector include,*** sharing personal information with third parties without consent for marketing purposes, stolen or lost banking number or card, sharing personal information or allowing access to third parties without informed consent, inadequate notification to an individual concerning what will be done with their data, collecting more personal data than is necessary, refusal to provide financial records upon request by client, incorrectly recording personal information, and loss of customers personal data due to improper security measures[15].

II. Authentication:

Encryption may help to make the transactions more secure, but there is also a need to guarantee that no one alters the data at either end of the transaction. There are two possible ways to verify the integrity of the message. One form of verification is the secured Hash Algorithm which is "a check that protects data against most modification." The sender transmits the Hash algorithm generated data[16].

The recipient performs the same calculation and compares the two to make sure everything arrived correctly. If the two results are different, a change has occurred in the message. The other form of verification is through a third party called Certification Authority (CA) with the trust of both the sender and the receiver to verify that the electronic currency or the digital signature that they received is real[17].

III. Divisibility:

e-banking increases security risks, potentially revealing up till now isolated systems to open and risky environments. Security breaches essentially fall into three categories; breaches with serious criminal intent (fraud, theft of commercially sensitive or financial information), breaches by 'casual hackers' i.e., defacement of web site s

[15] https://www.researchgate.net/.../283384799_E-Banking_Security_Issues
[16] https://www.researchgate.net/.../283384799_E-Banking_Security_Issues
[17] https://banking.apaccioutlook.com/.../data-security-and-privacy-concerns

or 'denial of service' causing web sites to crash, and flaws in systems design and/or set up leading to security breaches (genuine users seeing/being able to transact on other users' accounts).

All these threats have potentially serious financial, legal and reputational implications. Many banks are finding that their systems are being probed for weaknesses hundreds of times a day but damage/losses arising from security breaches have so far tended to be minor. However, some banks could develop more sensitive "burglar alarms", so that they are better aware of the nature and frequency of unsuccessful attempts to break into their system[18].

SECURITY AND PRIVACY REGULATORY ENVIRONMENT

Internet banking is a popular and convenient method of doing online banking transactions but there is no dedicated Internet banking laws in India. There is no doubt that Internet banking has proved to be a great enabler in India, with significant increases in transaction volumes each year. But just how secure are Internet banking websites in the country? There is no simple answer to this question. In fact, any answer at all will depend on the particular criteria used for evaluation. This discussion outlines the common vulnerabilities that many Indian banking websites seem to suffer from, and highlights gaps in Internet banking security. There is definitely scope for improvement, and a need for banks to standardize on security features for Internet banking overall. However, Reserve Bank of India (RBI) has been consistently making efforts to make internet banking transactions more and more secure. During the year 2010, Reserve Bank of India set up a Working Group under the Chairmanship of S.R.Mittal to address the Regulatory and Supervisory concerns[19] in i-banking (Now Electronic Banking) focusing on

i) Legal and regulatory issues,
ii) Security and technology issues and
iii) Supervisory and operational issues.

[18] https://www.thehindubusinessline.com/...banking/...systems...privacy-issues/article962
[19] https://rbidocs.rbi.org.in/rdocs/notification/PDFs/21569.pdf

Major recommendations of the Group accepted by RBI have been listed as under.

I. Technology and Security Standards:

A. Banks should designate a network and database administrator who will ensure that only the latest versions of the licensed software with latest patches are installed in the system
B. Banks should have a security policy duly approved by the Board of Directors.
C. Banks should introduce logical access controls to data, systems, application software, utilities, telecommunication lines, libraries, system software, etc. Logical access control techniques may include user-ids, passwords, smart cards or other biometric technologies.
D. At the minimum, banks should use the proxy server type of firewall so that there is no direct connection between the Internet and the bank's system.
E. PKI (Public Key Infrastructure) is the most favoured technology for secured Internet banking services.

II. Legal Issues

- From the legal perspective, security procedure adopted by banks for authenticating users needs to be recognized by law as a substitute for signature. In India, the **Information Technology Act, 2000**, in **Section 3(2)** provides for a particular technology (viz., the asymmetric crypto system and hash function) as a means of authenticating electronic record. Any other method used by banks for authentication should be recognized as a source of legal risk.

- In Internet banking scenario, there is very little scope for the banks to act on stop-payment instructions from the customers. Hence, banks should clearly notify to the customers the timeframe and the circumstances in which any stop-payment instructions could be accepted.

- The **Consumer Protection Act, 1986** defines the rights of consumers in India and is applicable to banking services as well. Currently, the rights and liabilities of customers availing of Internet banking services are being determined by bilateral agreements between the banks and customers. Considering the banking practice and rights enjoyed by customers in traditional banking, banks' liability to the customers on account of unauthorized transfer through hacking, denial of service on account of technological failure etc. needs to be assessed and banks providing Internet banking should insure themselves against such risks.

III. Regulatory and Supervisory Issues[20]:

As recommended by the Group, the existing regulatory framework over banks will be extended to Internet banking also. In this regard, it is advised that:

1) Only such banks which are licensed and supervised in India and have a physical presence in India will be permitted to offer Internet banking products to residents of India. Thus, both banks and virtual banks incorporated outside the country and having no physical presence in India will not, for the present, be permitted to offer Internet banking services to Indian residents.
2) The products should be restricted to account holders only and should not be offered in other jurisdictions.
3) The services should only include local currency products.
4) The 'in-out' scenario where customers in cross border jurisdictions are offered banking services by Indian banks (or branches of foreign banks in India) and the 'out-in' scenario where Indian residents are offered banking services by banks operating in cross-border jurisdictions are generally not permitted and this approach will apply to Internet banking also.

   The existing exceptions for limited purposes under FEMA i.e. where resident Indians have been permitted to continue to maintain their accounts with overseas banks etc., will, however, be permitted.

[20] https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR101787145DFC87BC4D08B7E932309D587701.PDF

5) Overseas branches of Indian banks will be permitted to offer Internet banking services to their overseas customers subject to their satisfying, in addition to the host supervisor, the home supervisor. As per revised guidelines, no prior approval of the Reserve Bank of India will be required for offering Internet Banking services.

Further, The Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (2010) was constituted[21], under the Chairmanship of Shri G.Gopalakrishna, Executive Director, RBI. The Group examined various issues arising out of the use of Information Technology in banks and made its recommendations in nine broad areas. These areas are: **IT Governance, Information Security, IS Audit, IT Operations, IT Services Outsourcing, Cyber Fraud, Business Continuity Planning, Customer Awareness programmes and Legal aspects**. Final guidelines in the respective areas as mentioned above were issued to banks for implementation.

CONCLUSION:

The internet has grown exponentially; the number of Internet users stood at **481 million** in December 2017, an increase of **11.34**% over December 2016 said the report titled, Internet in India[22]. E-banking services play a vital role in improving much Customer satisfaction. It has its own impact on customer satisfaction. Security is the most significant issue in online banking.

It may arise in form of risk in case of unauthorized access of key information of bank account Many people are still not comfortable with online portals, especially from the security point of view. In addition to this, banks also face the internal problems like employee frauds. Trust of customer in a web venture is an important concern. Many customers hesitate to deal with an online banking as they are not sure of the quality of products and services they will receive. Banks may encounter problems due to wrong choice of technology, insufficient control

[21] https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WREB210111_ES.pdf

[22] https://economictimes.indiatimes.com/tech/internet/internet-users-in-india-expected-to-reach-500-million-by-june-iamai/articleshow/63000198.cms

processes and inappropriate system design. Inappropriate technology may lead to a loss in terms of financial loss as well as loss, of brand image and goodwill.

It is clear that if any bank offers e-Banking services with best security measures, definitely it leads to reach maximum level of customer satisfaction[23]. Electronic banking is offering its customers with a wide range of services. Customers are now able to interact with their banking accounts as well as make financial transactions virtually from anyplace without time restrictions.

e-Banking is offered by many banking institutions due to pressure from competitors. The future of electronic banking will be a system, where users are able to interact with their banks "worry-free" and banks are operated under one common standard. Most research studies have indicated that the common problem affecting information security and privacy of customers is e-services provider's lack of security control which allows damaging privacy losses. Apart from that, another problem is the subsequent misuse of consumers' confidential information, as in identity theft. These may affect customer's confidence toward online business transaction in a variety of privacy risk assessments by consumers. Current technology allows for secure site design. It is up to the development team to be both proactive and reactive in handling security threats, and up to the consumer to be vigilant when doing business online.

Reference

1. M L TANNAN, Banking Law & Practice in India, 27th Edition, Volume 1,2,3
2. Rajneesh De and Padmanabhan, Chitra, (2002), "Internet Opens New Vistas for Indian Banking", Express Computer, 16th September, available at http://www.expresscomputeronline.com/20021202/banks1.shtml. Accessed on 9th October, 2018.
3. RBI (2012), Report on Trend and Progress of banking in India.
4. RBI guidelines on Internet Banking.

[23] https://www.researchgate.net/.../283384799_E-Banking_Security_Issues

https://www.rbi.org.in/SCRIPTs/NotificationUser.aspx?Id=414&Mode=0

5. RBI's Report of Internet banking (2001) available at http://rbidocs.rbi.org.in/rdocs/notification/PDFs/21569.pdf
6. Reserve Bank of India (2001), Report on Internet Banking, Available http://rbidocs.rbi.org.in/rdocs/PublicationReport/ Pdfs/21595.pdf Accessed on 9th October, 2018.

FLAWS IN e-BANKING – A PREY TO CYBER HUNTERS

R.B. Rishabh*
&
B. Yamuna Saraswathy

ABSTRACT:

The term e-banking is a contemporary term which derives its origin from the recent past. Banking products and services are provided by e-banking through Information Technology (IT). The ever-growing IT has led to the speeding up of banking transactions increasing effective communication between bank and its customers. To add on, the cut-throat competition has pushed the banks to adopt e-banking concept.

Though the e-banking system has got couple of merits, it is not free from security threats. To be particular, the online banking accounts are mostly falling as a prey to cyber hunters. These cyber hunters are instigated as the e-banking products and services have opened a gateway to information on millions of people. This ultimately results in the infringement of privacy of customers by cyber hunters. There is, therefore, a need to implement stringent cyber-security measures to protect the privacy of the customers.

This article aims to cast light upon the concept of electronic banking and various security threats in e-banking sector. The paper also analyses how these security threats infringes the privacy of the customers. Further, it statistically analyzes the recent e-banking breaches. The authors give an insight about the regulatory and legal framework with regard to e-banking crimes and provide suggestions for betterment of such laws.

INTRODUCTION:

Electronic banking (e-banking), a relatively new term to the Indian society, owes its emergence to Liberalization, Privatisation and Globalisation (LPG) movement which has freed the society from the clutches of regulations of the government. In the current scenario the

* Students, School of Excellence in Law, TNDALU.

impact of Information Technology (IT) is crucial in any service oriented industry and the banking industry stands no exception to it. Gaining access to information technology is to be regarded as a major contribution to the growth of e-banking field. E-banking services have reduced cost and workload to its customers and branches respectively. At present, all major banks provide e-banking services which have brought in cut-throat competition in this industry. Though the fruits of information technology taste good, the rapid developments in the technological perspective of the banks have to cope up with the high compliance costs. e-Banking is gaining pace in the developed and as well as developing countries. The products of e-banking technologies such as Automated Teller Machines (ATMs), internet banking, mobile banking etc., have proved to be a revolution in the contemporary banking system. Through e-banking, the customer will have all details of his/her accounts on his palm. E-banking has contributed to safeguarding the environment as well by going paperless. Nowadays, people rely more on information provided by digital applications than the information rendered from the people which signifies increasing faith in information technology. Although the e-banking services have reduced the visit which each customer makes to their banks, the physical branches of the bank cannot be completely replaced by e-banking products, because every customer expects a personal touch while availing banking services. Banks have moved on to the Core Banking Solutions (CBS) and back office of the banks has been shifted from the branches to a centralised zone. The e-banking products have been designed to function 24/7, which really tests the ultimate potential of the information technology. The advent of Information Communication Technology (ICT) has opened the cyber space so that it could be infringed by cyber criminals. The more and more the systems are breached, more and more Personal Data Information (PDI) are acquired by the cyber hunters. So, we can come to a conclusion that privacy of the internet users are at stake. In recent years the number of cyber crimes has drastically gone up. E-banking activities are being regarded as a lucrative prey for criminal activities and now the cyber criminals have been practicing sophisticated techniques to hunt the e-banking sites or applications. The main reason why cyber criminals consider e-banking as a lucrative prey is because of the increasing

number of users who are accessing these sites and applications. The main concern relating to the insecurity in e-banking service is that this sector lacks the awareness from the regulatory authorities. The Government has to either make the available laws pertaining to security of e-banking stringent; or to come up with an exclusive law so as to ensure the security of e-banking products and services. The basic idea behind the cyber hunters is to procure the personal data information in order to commit cyber crimes pertaining to data such as identity theft, cyber stalking, site cloning etc. They don't just indulge data related crimes but also commit cyber terrorism through software related means such as Trojan, spyware, hacking, phishing, smishing, vishing, spamming, spoofing, salami attack, money laundering etc. Whatever be it, the trend of people availing the e-banking services has not come down amidst the cyber hunters.

EVOLUTION OF E-BANKING:

e-Banking is the process of using the internet to organize, examine, and make changes to bank accounts, investments, etc[1]. The term 'e-banking' was first arisen in 1980s and it became famous only in the mid 1990s. During its foundation years, the usage of e-banking was through a telephone line. It was first in the US where the banking services in an online mode were used using the video tech system. In UK, a system known as Prestel System had used a computer to link to a telephone line and a television set. Earlier, online banking was provided with an option for only a couple of services such as payment of gas, electricity and phone bills.

The success of e-banking depends upon customer's adoption of it. In the beginning, even setting up of a webpage to provide details or information regarding the products and services of the bank was considered as internet banking. Presently, in an advanced level, it provides various facilities such as transfer of funds, buying of shares and insurance, accessing different accounts etc. The most exciting advantage of internet banking is that all the services can be availed in a blink of an eye. Through e-banking one could pay taxes, book railways and air tickets, buy products online, apply for loans etc.

[1] Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/electronic-banking.

Thulani had identified three functional levels of internet banking which are informational, communicative and transactional.[2] Under *informational level*, the banks have provided the marketing information on a standalone server regarding bank's products and services. Here in this case, the risk under information system is very low since there is no established link between bank internal network and the server. Under the *communicative level of internet banking*, there exist interaction between the customer and the bank's system. The last but not the least, being the transactional level of internet banking which facilitates a customer of a bank to transfer funds from one account to other person's account, pay bills etc. In this level of internet banking, the risk involved is pretty high compared to the other two levels of internet banking. Therefore, the security measures at the transactional level of internet banking have to be tightened so as to safeguard the information of such accounts of customers from the cyber hunters.

TECHNIQUES OF CYBER INFRINGMENT:

The 21st century can also be called as an internet era as the use of digital space is flourishing in all the sectors. Once we start using the internet and cyber space, there is no real exit as all our information is stored infinitely. The more the usage of digital space, the more is the threat to cyber security. For this reason, the electronic banking has proved to be an easy and lucrative target to the cyber fraudsters. The cyber attacks on e-banking sector have increased rapidly in recent years as the use of online banking systems by people has increased only in the past few years. To reduce these threats and to safeguard customers, the banks should adopt stringent cyber security systems and other preventive measures. But first of all, one should understand the types of cyber attacks in e-banking sector for controlling them. In this paper, various types of cyber threats in e-banking sector are discussed.

1) Phishing:

Phishing is one of the classic cyber attack methods which use spoofed emails or messages that leads the user to infected websites to

[2] Thulani D, Tofara C, Langton R, Adoption and Use of Internet Banking in Zimbabwe: An Exploratory Study. Journal of Internet Banking and Commerce, (2009).

obtain the bank information from people such as account number, credit/debit card number, passwords, social security number etc. These mails are designed to appear as authenticated ones so as to fraudster people easily. Thus ultimately, the hackers can access the victim's bank account effortlessly.

2) Vishing:

Vishing is a combination of voice and phishing where the cyber hunters use voice calls and represent themselves as the employees of banks and thereby making the bank's customers to provide all the information related to their account.

3) Smishing:

Smishing is a combination of SMS and phishing. It is more like vishing, but here the cyber criminals collect bank information from the customers by sending SMS and making them believe it as authenticated message from the banks.

4) Watering hole:

Watering hole attack is merely a development from phishing, attack. In phishing the hackers attack people by sending spammed mails which connects people to infected websites, whereas in watering hole, the cyber attackers compromise a particular website and wait for people to access such websites. This type of attack targets only a specific group of people and the hacker has to wait for months after infecting such websites.

5) Pharming:

The term 'pharming' is derived from two words namely 'farming' and 'phishing'. Here the cyber criminals hack the URL of a bank website thereby redirecting such bank customer to a fake bank website. And it will be really difficult for the customers to differentiate between the original and fake website and so they usually end up providing their information in such websites. Hacking of a bank's URL can be done in two ways:

1. DNS Cache Poisoning

2. Hosts File Modification

6) Assault by Threat:

When a person is threatened of his life or lives through e-mails, messages or calls to give his bank details, it is known as assault by threat.

7) Credit Card Redirection:

This is a new type of cyber attack in e-banking which compromises the e-commerce websites thereby getting access to the credit card information of such website's users. Here, the credit card processing file is modified and the details of such credit cards are redirected to a phishing site during the payment process when used in the particular e-commerce website.

8) Carding:

One of the easiest ways to get access to people's money can be done by carding. Carding is a method in which the cyber fraudsters create duplicate ATM cards and thereby use it whenever they need money without the knowledge of such victim.

9) Skimming:

This is also a form of stealing the card's information by way of using sophisticated devices to capture cardholder details from the magnetic strip available in those cards. This is done during ATM transaction process and at the end the personal details will be downloaded by the cyber fraudsters.

10) Triangulation:

In this form of cyber attack, the hackers create an infected commercial website providing huge amount of discounts and free shipping of its goods. When an individual buys the products using the bank cards in such e-commerce sites, the hackers collect all the information of such cards effortlessly.

11) Malware Attacks:

Malware is a kind of software that bugs a person's computer and spreads viruses through mails and social networks to other computers. This bug/virus will be controlled by the hacker and the information found in such computers will be compromised. This is one of the most dangerous cyber attacks as this is mostly used for demanding ransom from individuals. So when this type of attack is made on a banking system, it ultimately compromises the customer's information available. Some of the well known banking malware are Zeus, Carberp, Spyeye, Tinba and the recent KINS. But surely, the first three agents are considered to be the most serious threats by the security community. Zeus is the oldest of them. Numerous variants were detected during the last five years, and they have been often used to commit cyber fraud on a large scale. The first version of the Zeus Trojan was detected in July 2007, when it was used to steal information from the United States Department of Transportation.[3] This type of cyber attack on the governments is said to be cyber warfare or cyber terrorism.

12) Scareware:

The cyber criminals scare away the individuals and force them to download particular software which ends up in compromising and stealing of such person's information. This type of cyber attack is known as scareware.

13) Man in the Browser (MITB):

Man in the Browser is a type of software or an infected code which attaches itself to the computers in banks and helps the hackers to modify the banking transactions of the people to their interests. This type of attack can be hidden from the victims and it will be very difficult for both the bank and the individual to figure out that such type of attack has been made.

14) Salami Attack:

Salami attack is a sophisticated form of cyber attack in banking sector where hackers make small attacks which end up in accumulating a large amount of money in the end. It is also known as

[3] *Modern Online Banking Cyber Crime,* INFOSEC INSTITUTE, (Nov 5, 2013), https://resources.infosecinstitute.com/modern-online-banking-cyber-crime/.

salami slicing. In banking sector, the attackers hack the bank accounts of people and deduct very minimal amount from it for a specific period of time. This makes the detection of such cyber attack difficult and the bankers and victims are always unaware of such attacks.

IMPACTS OF CYBERCRIME:

The digital era has proved to be of immense help for the growth of business organisations. Banking institutions being a lucrative business had to adopt digitalisation for promoting its business. While digitalisation has many benefits, it is not free from the dark side of cybercrime. Since the banks have all the information of customers from personal identification to bank account details, it is easy for the cyber hunters not only to earn huge amount of money but also infringe the privacy of such customers by way of identity theft. Nevertheless, the impact of such cybercrimes still remains to be a nightmare. Some of the impacts of cybercrime are discussed below.

Financial Impact:

It is a known fact that the main motive of cyber hunters is earning money. When the bank servers are hacked, it can result in huge monetary loss as they get all details including debit/credit card number with the Personal Identification Number (PIN). Not only this, the banks have to spend huge amount of money to identify the origin of such threat and recover from it.

Social Impact:

The cyber attacks not only results in financial loss but also creates a greater impact on the society. This is because when there is a cyber attack, the customer loses trust over such bank which ultimately damages the reputation of the financial institution. This also results in loss of productivity and customer confidence in the banks.

CYBER SECURITY TRENDS IN INDIA:

At present age, information is considered to be a valuable asset and storing of such information in data warehouses and clouds have made the work of service sectors easier. However, the development of cyber space poses a great threat to such information asset. With the

evolving concept of digitalisation, the information of every single person from physical address to social security number is available online. Therefore, increasing the data security system in all the sector remains the sine qua non of protection of such valuable information. As for as the banking sector is concerned, ensuring the digital information security has become vital.

Indian banks are not an exception to these cyber frauds/attacks. They prove to be a lucrative target for the cyber criminals as they provide large amount of information data. In this regard, the Reserve Bank of India has issued certain guidelines regarding cyber security frameworks in banks through two notifications so far.

(i) The first notification was issued on April 29, 2011 by the Department of Banking Supervision regarding Information Technology, E-Banking, Technology Risk Management and Cyber Frauds.[4] It directed the banks to create a separate Information Security Team to focus on the data security and cyber frauds. The circular also mandated the banks to have control over the access of IT data even by its employees as the data can also be breached due to insider attack or espionage. It made the banks to assess the vulnerabilities soon after they find them and protect the data so as to avoid any form of cyber attacks. Other security measures such as encryption, protection against malware, and developing robust firewalls were also provided in the circular. The report discussed about the awareness to be created among the employees regarding growing cyber threats and ways to track such cyber frauds.

(ii) Even with all the above mentioned mandates and increased security levels by banks, the cyber crimes were not under control as the technology used by the banks has further gained momentum. This made the RBI to issue another special circular on Cyber Security Frameworks in Banks on June 2, 2016.[5] This circular mandated the banks to have a board approved cyber security system and to give an

[4] Department of Banking Supervision, RBI, *Guidelines on Information Security, Electronic Banking, Information Risk management and cyber frauds,* THE RESERVE BANK OF INDIA, (Apr 29, 2011), https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf.

[5] Reserve Bank of India, *Cyber Security Frameworks in India,* THE RESERVE BANK OF INDIA, (Jun 2, 2016), https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0.

immediate notice to RBI of the cyber attacks, if any. The circular directed the banks to have a continuous surveillance over IT data and to create cyber awareness at all levels, including top management authorities and stake holders. The banks were also directed to increase its defence levels in the cyber space.

(iii) Still, the cyber attacks haven't come down. As the technology develops, the landscape of cybercrimes and cyber warfare are also increasing. Therefore, RBI has included cyber security measures in its agenda for the year 2018-19. Since the digital payments in the banking sector has gained popularity among the public, the RBI has decided to further strengthen and modify its encryption levels, cyber security and Know Your Customer (KYC) norms. The RBI report for 2018-19 said that, "In order to secure consistency and improve the efficiency of the offsite monitoring mechanism, an Audit Management Application portal to facilitate various supervisory functions of the **Cyber Security and Information Technology Examination (CSITE)** Cell and to fully automate monitoring of returns has been envisaged, which will be operationalised by March 2019"[6].

The precautionary systems adopted by the banks in the recent years are as follows:

- Having a proxy server type of firewall so as to provide for high level of monitoring as there will be no direct connection between the internet and the bank's system.
- Usage of Secured Socket Layer (SSL) by the banks provides authenticated servers by using client side certificates issued by the banks. Nowadays most of the banks use 128-bit SSL for securing the online transactions and communications. In India, only SBI uses 256-bit SSL for protecting the communication servers.
- Having proper infrastructure for backing up of data by the banks is crucial.

[6] PTI, *RBI working on measures to further beef up cyber security in FY19,* THE E.T., Sep, 03, 2018, https://economictimes.indiatimes.com/news/economy/policy/rbi-working-on-measures-to-further-beef-up-cyber-security-in-fy19/articleshow/65656064.cms.

- Record keeping of the online applications such as mobile banking apps in encrypted and decrypted form.

SUGGESTIONS:

Before 1980s, the cyber attacks were lesser in number and committed by individuals, mostly by computer nerds who wanted to prove their knowledge. But in later years, the cybercrimes became more organised and sophisticated, as it was found to be a lucrative field for committing crimes. The shift from mischievous threats to properly organised and targeted attacks has created a greater concern among the organisations and governments worldwide. Hence, there is an exigency to address both security and privacy issues prevailing in the banking institutions.

(ii) Firstly, it is pertinent to understand that launching of cyber attack does not cost much, but the identification of such crimes cost huge amounts of money. In the digitalised and globalised world, any anonymous person can launch cyber attacks on a banking institution in one country residing in a completely different place. This makes the tracking back of such attack difficult and costly. Thus, fighting such cybercrime single handedly is almost impossible. So the governments and business organisations across the world must work together and address this problem by way of regulating the cyber security in a cross-border or universal manner.

(iii) Secondly, while strengthening cyber security is significant it is also important to sail safe in the cyberspace. Awareness must be created among the customers regarding the cyber threats so as to protect themselves from the cyber hunters.

(iv) Thirdly, special legislations regarding cyber security in banking must be enforced. Not just enforcement, implementation of such laws is crucial thereby not only taking actions against cyber attacks, but also taking preventive measures before such attack is made.

Finally, special cyber cells dealing with the cyber attacks must be organised in each and every bank so as to control the cyber threats. The only possible way to prevent the organised cyber attacks is to have a cyber security mechanism in an organised manner.

CONCLUSION:

Even though e-banking services in India have been gaining pace, the rate of adoption is still comparatively low considering the developed countries. The Indian banks have also invested huge amounts to boost the e-banking activities so as to facilitate the customers and in return get their loyalty towards the banks. Though there are various factors which restrict the customers from using e-banking services, the main concern remains the concern for security and privacy. In India, legislations which pertain to the security of e-banking are shed under the Information Technology Act, 2000[7] and are scattered under the SEBI Regulations, Reserve Bank of India's guidelines in order to safeguard privacy, especially online privacy, in electronic banking system. Moreover, the 2008 amendment of the Information Technology act has provided special provisions under sections 43, 43A, 44, 66E, 67, 67A, 67B and few other sections which promotes and protects data and privacy in online transactions. The e-banking services are mainly availed by the younger generation and even today the older generation feels the usage of e-banking to be a threat. E-banking services in the near future must be designed in such a way that irrespective of who the user is, there will not be any sense of difficulty or dismay using these facilities. Though we talk about the infringement of privacy on the PDI's of the customers, yet we've no other means other than e-banking to transact in a speedy manner. Hence, the Government should come up with methods of securing the information and the people through various security mechanisms, which would protect the customers from threats of external source and it should also bring in penal/stringent provisions, which would deter the employees of the organisation from taking part in unscrupulous activities such as leaking of information, etc.

[7] Information Technology Act, No. 21, Acts of Parliament, 2000 (India).

CONSUMER PROTECTION ACT AND BANK'S LIABILITY – AN ANALYSIS

J. JAMES JAYAPAUL*

ABSTRACT

The Customer of a bank is regarded as a valuable customer. The Bank is the provider of service to the customer. According to the Consumer Protection Act, 1986, if there is a deficiency in service by a service provider, the bank is liable to the customer. So the banks are also brought within the purview of Consumer Protection Act. Though the parliament of India has framed many laws for the protection of interest of customers in banks, the ultimate remedy to the full satisfaction is awarded only by the consumer forums. Since in the modern technological society when many errors are committed by bank authorizes affecting the rights of the customers, the role of consumer forums is appreciable. Every Indian citizen is having an account in the bank and therefore the chances of creating more frauds are possible. The Consumer forums only question the unfair deficient act of the bank authorities. Though the remedy through the Ombudsman scheme is available, majority of the decisions go in favour of the bank only.

Some examples of deficiency on the part of the banks are, the failure to return matured deposits, the wrongful dishonour of cheques, the matters concerning the eligibility of parties to any credit assistance, causing undue delay in releasing the instalments of the sanctioned loan, the Charging of interest at a rate higher than the rate stipulated in the loan agreement, the refusal to return the security documents even after repayment of the whole loan etc.

In this article the various negligent acts of the bank officials are pointed out and the decisions of the State Commissions, the National Commission, and the Supreme Court (the final authority), on different aspects of banking and other services offered by banks are analysed.

* M.A., M.L., Asst. Professor /Research Scholar

The growing interdependence of the world economy and international character of many business practices have contributed to the development of universal emphasis on consumer rights protection and promotion. Consumer rights are the rights given to a "consumer" to protect him/her from being cheated by salesman/manufacturer. Consumer protection laws are designed to ensure fair trade competition and the free flow of truthful information in the marketplace. These laws were designed to prevent businesses that engage in fraud or specified unfair practices from gaining an advantage over competitors and may provide additional protection for the weak and those unable to take care of themselves. Consumer Protection laws are a form of government regulation which aim to protect the rights of consumers. The customers of bank are also coming within the term consumer.

There have been many reforms in the banking sector like dilution of government stakes, deregulation etc that resulted in greater competition. Nowadays, banking has moved from class to mass and this has resulted in numerous problems. But more attention also needs to be given to consumer protection in regard to the banking sector.

In the Constitution of India, social and economic justice is an important part in which the consumer justice and protection is also a part. There were number of legislations passed by the Indian Parliament such as Drugs (Control) Act, 1950; Prevention of Food Adulteration Act, 1954; Essential Commodities Act, 1955; Essential Services Maintenance Act, 1968; Trade and Merchandise Marks Act, 1958; MRTP Act, 1969, etc. But these entire Acts failed to protect the interest of small consumers. The procedures under these acts are elaborate and litigations also time consuming and costly. The United Nations General Assembly passed a resolution No.39/248 on 8/4/1985 adopting guidelines relating to consumer protection, which further provide a framework for the Governments of the developing countries, for formulation of consumer protection policies and legislations. Finally in 1986, the Indian Parliament passed the Consumer Protection Act, 1986, to protect the interest of the consumers and to provide them a mechanism for easy, quick and cheap redressal of grievances against the mighty and unscrupulous producers/traders and service providers.

According to the Act, the definition of the term "Consumer", under section 2(1)(d) of the Act, includes a person who hires or avails of any service for a consideration. Therefore in banking transactions, a customer of a bank who has a bank account with the bank, or a person who purchases a bank draft, hires locker facility or obtains bank guarantee from a bank are all "consumers". They can prefer complaints under the Act for "deficiency in service" on the part of the bank or for "restrictive trade practice" or "unfair trade practice" adopted by the bank. Competition helps consumer because it promotes choice, helps bring quality services or products at low rates by reducing inefficiencies. There is reduction in the cost of banking services and consumers need to make use of the facilities available in the changing environment to avail the reduced cost, like use of ATMs, internet or telephone banking.

The Complaint redressal mechanism already in existence are :

1. The code of Banks commitment to Consumer (2006).
2. Fair practices code for Lenders (2003).
3. The in-house complaint redressal mechanism set by banks.
4. Ombudsman office.

But the consumers of banks are not awarded suitable compensation. Hence they are approaching the consumer courts.

In this article, the author will analyse different case laws concerning bank and its customers.

Issue of Law and Fact.

In *Awaz Punita Society Vs. Reserve Bank of India*, AIR 2008 (NOC) 2528, there was delayed information regarding dishonour of cheque. The Drawer claimed compensation. Held, the dispute requires recording of evidence. Therefore, suit alone can determine the remedy and not the consumer forums.

Higher Interest in Credit Cards

In *Don Valley Rice Ltd. Vs. SBI,* (2003) 2 CPJ 196 (NC), the Bank charged higher rate of interest to credit card holders, for failure to make full payment on due date. Held, it amounts to unfair trade practice and banks are liable to return the excessive interest.

Sanctioned Loan not Disbursed

In *Raj cello cham products (P) Ltd. Vs. Punjab & Sind Bank*, AIR 2009 (NOC) 2925 NCC, the claim for a loss caused by the bank's failure to disburse the sanctioned amount of loan cannot be adjudicated by a consumer forum. Since the matter contains both question of law and fact, the civil courts will be the proper deciding authority.

After Stop Payment Notice , Cheque amount disbursed

In *Bank of India Vs. Dr. Mukesh Kumar Shukla*, 1993 CPJ 472 MP, the bank after receiving stop payment notice from the account holder, still made payment negligently. It was held that, it is a Deficiency in service and the bank was directed to pay compensation.

Bankers Duty towards proper collection of cheques

In *Canara bank Vs. Uppal brass industries,* (1997) 2 CPJ 143, bank issued crossed cheques in favour of a firm. The firm did not receive the cheques. The Account statement of the customer showed that the cheques were cleared. Held, that it was deficiency in service.

Informing customer for returned cheque

In *SBI Vs. Rajendar Lal,* (2003) 4 CPJ 53 (NC), a cheque was dishonoured. During the transit it was lost. Held, the bank is liable for deficiency in service and awarded Rs.15,000/- compensation to the customer.

Realisation of shares deposited for loan due

In *R.D.Chinoy Vs. Central Bank of India*, (1992) 2 CPR 663 (NC), the bank was holding shares as a security. It sold them for realisation of loan amount for lesser value. Held, it was deficiency of service.

Failure to return security after loan closure

In *S.K.Bhatia Vs. Punjab National Bank*, (1996) 3 CPJ 375 HP, the Consumer Court awarded Rs.50,000/- as compensation to the consumer on the ground that the bank had not returned the mortgaged jewels after payment of loan amount for 14 years. It is a huge loss for the mortgagor.

Sale of pledged articles

In *South Indian Bank Vs. Tamilnadu Consumer Council*, (1992) 1 CPJ 299, the pledged jewellery was sold before the expiry of notice period. Held, that it is deficiency of service.

Bank Employees strike

In *Consumer Unity & Trust Society Vs. Bank of Baroda,* (1992) 1 CPR 837, it was held that if the bank employees are on strike and the consumers are affected, then it can be deemed to be a deficiency in service. But the Supreme Court in appeal held that if there is no loss for a consumer, then it is not a deficiency in service.

Recovery by unwarranted force by the Bank Agent:

In HDFC Bank Limited vs Balwinder Singh, [III (2009) CPJ 40 (NC)], the complaint was of the bank, or its loan recovery agent, employing musclemen to take forcible repossession of the hypothecated vehicle and thus causing physical harassment and mental trauma to the complainant. The District Forum allowed the complaint and directed the bank to pay compensation of Rs.4 lakhs for repossessing the vehicle in this manner and reselling it to a third party. The State Commission confirmed the order in appeal. Dealing with the bank's revision petition, the National Commission expressed shock that the bank had hired musclemen directly or through its recovery agents to recover the loan/repossess the vehicle. The Commission also referred to the State Commission's order, which had observed that the alleged letter produced by the bank purporting to the complainant voluntarily handing over possession of the vehicle was unreliable and that no notice was given to the complainant at the stages of repossession and sale of vehicle. In dismissing the petition, the Commission relied upon its judgment in Citicorp Maruti Finance Limited v S.Vijayalaxmi [III (2007) CPJ 161 (NC)], where it had strongly deprecated such practices. The Commission

dismissed the petition and awarded Rs.25,000/- as exemplary costs in this case.

Opening of Locker without prior permission of the Customer:

In Ist Appeal 7/1991 decided by NCDRF, the locker of the customer was not opened for a long time. After some years, a relative came and requested the bank authorities to open the locker. Without verifying the legal heir certificate, the bank opened the locker and handed over the contents. It was held by National commission that it is Deficiency in service and the bank is liable to legal heirs.

Ensuring safety of the money to be deposited by a customer inside the bank premises is part of service rendered by a bank to a customer.

In *Col.D.S.Sachar Vs. Punjab & Sind Bank*, 2003 CPJ, the Customer bought money to be deposited in his account. A person stole his money inside the bank and ran away. The complaint was allowed with direction to the respondent-bank to pay amount of Rs.45,000/- with interest at the rate of 9% per annum from the date of filing of complaint and cost of Rs.5,000/-.

Mortgaged Documents not returned immediately

In *Harikunmar Raju Vs. ICICI Bank*, 2014 CPJ, the borrower had repaid the loan amount, but the original mortgaged documents were not returned for about 5 years. Held, it is deficiency of service.

Bank directed to compensate the consumer for making payments on wrong signatures

In *Udayasanker Vs.Central Bank of India*, 2011 CPJ, the signature in the cheque was forged, but the bank did not notice the difference and took the defence that the customer could have given stop payment instructions. Held, it is a deficiency in service.

Controversy between SARFAESI Act and Consumer Protection Act

In *Punjab National Bank Vs. Consumer Disputes Redressal Forum,* AIR 2012 Kerala 8, the petitioner bank sanctioned a loan to the party.

When the party defaulted the amount, the account was classified as Non-Performing Asset by the Bank. Proceedings initiated under SARFAESI Act. The borrowers moved under Consumer Protection Act on the basis that the action of the bank has to be stopped since there is a consumer dispute. They contended that banking is a 'service' and there had been a deficiency of service on the part of the Bank.

So the issue was whether the Consumer Forum has jurisdiction to entertain a matter which is under SARFAESI Act proceedings. There was also a question with regard to applicability of Section 34 of the SARFAESI Act where civil court's jurisdiction is barred.

The High Court of Kerala clarified the position in favour of SARFAESI Act. The Court rested its finding on the following points:

The Consumer Protection Act is a general statute, whereas SARFAESI Act is a special enactment. A special enactment will prevail over the provisions of a general statute. No injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under SARFAESI Act. SARFAESI Act provides a remedy for the actions of the bank or other financial institution under Section 17. SARFAESI Act is a later enactment compared to CP Act. The provision of SARFAESI Act which excludes the jurisdiction of authorities to grant injunction against the proceedings under the Act should apply in equal measure to the Consumer Disputes Redressal Forum also. The High Court also took note of the issue of economic stability when there is blockade of large sums of money by unnecessarily causing hindrance to the recovery measures initiated by the Banks and other financial institutions. Therefore, SARFAESI Act overrides Consumer Protection Act.

CONCLUSION

Analysis of the various judgments of the Consumer Courts reveals that they have not only been awarding the loss for deficiency in services but also the compensation for the mental agony and harassment. By and large justice appears to have been done under the aegis of the

Consumer Protection Act, 1986 and to that extent it can be claimed that the Act has protected the interests of consumers.

PRIVACY IN BANKING TRANSACTIONS

Yuvasree. P.*

ABSTRACT:

This paper views the legal obligations of the banks to preserve the privacy issues in transactions of the customers. Also the consequences when the bank violates the principles laid down by the legislation and the judiciary to keep up the confidential information of the customers. The author tries to enlighten the circumstances with the help of certain cases in order to clarify that the infringement made by the banks not only lead to the punishments and payment of fines but also interrupts the trust of the people on such financial institutions, which paves the way for the loss of reputation of that institute. The author also provides certain suggestions for the banks regarding the enhancement in the protection of the sensitive information of the customers from the hackers and third parties. The author also tries to explain the role of the Government and the Legislature in the conservation of privacy issues in banking transactions. In addition, the author explains whether there are sufficient safeguards for the customer's privacy in the banks in India. The paper provides valuable information concerning the vital role of the legislation and the judiciary in the protection of the privacy in the banking sectors. The paper also attempts to compare the privacy issues of the banking transactions in India with other countries. The main aim of the paper is to find out the present situation of the banks in protecting the privacy issues of the customers.

INTRODUCTION:

Today with the fast moving technological development, each and every sector is advanced and workers are replaced by the machineries. But the banking sector could not be replaced by any other machinery and it continues to play a vital role from the 18th century. Though there are some negative comments about the banks, it is a matter of pride that many of the banks in India still act as the largest and the oldest banks. Generally banks have certain legal obligations and principles to

* B.A. LLB (Hons), II year, School of Excellence in Law, Taramani, Chennai-13.

follow; such principles and duties are laid down by the legislature and the judiciary. Also the customers have certain duties and responsibilities towards the bank.

In this paper, the author discusses the current status of the privacy in the banks, the role of the legislations and the judiciary in protecting the privacy of the customers in the banks, how the banks take measures to safeguard the customer's privacy, the situations when the customers get embittered easily and some suggestions for the banks to prevent the customers from being cheated.

(Here the banking includes both the online and offline banking in India)

PRIVACY IN BANKING:

The Data Privacy is a wide concept which deals with the privacy of the customers in various sectors like companies, banking, even social media etc. where the personal data of the customers have been collected for safety purposes but then such confidential information has been misused by some people for their own benefits. But in case of the banks and financial institutions, it is the responsibility of the banks to preserve the sensitive information of their customers.

One among the three organs of our State is the Legislature, which has its own significant function that is to make the laws for the welfare of the people and development of the country. There are numerous Acts which have been enacted for the protection of the privacy of the customers in banks. The Government has also provided the public with sufficient number of schemes to protect their privacy during banking transactions. As we all know, the judiciary plays its great role in preserving the privacy of banking customers.

Some of the acts enacted by the Legislature and the measures for the protection of the privacy of the customers in banking transactions are:

- **Banking Regulation Act, 1949**

  This Act is to regulate and supervise the banking firms in India by providing them with certain responsibilities and rights. If the bank breaches the privacy or confidentiality of their customers either accidentally or deliberately, then the complaint can be filed and it is considered as valid.

- **Social Security Act, 1964**

  This Act provides financial assistance and ensures financial support for the people and protects them by providing security not only in India but also in other countries like U.S.A.

- **Consumer Protection Act, 1986**

  The Act provides each and every consumer with certain rights in order to prevent them from being cheated. It also punishes the wrongdoers with compensation and in some cases with fine and imprisonment for those who engage themselves in fraudulent activities to swindle the consumers.

- **Privacy Act, 1993**

  This Act affords the banks with legal obligations and principles to follow. There are some 12 principles in case of the personal information. In this particular Act, the complaint can be filed against the lawbreaker to the Privacy Commissioner and compensation is provided as the remedy. It controls the behaviour of the staff member in the banking sector and not the action of the banks.

- **Companies Act, 1993**

  It protects the confidential information of the customers with the company liquidator in the companies.

- **Tax Administration Act, 1994**

  It is to re-enact the administrative provisions in the Income Tax Act 1976 and to re organise the Inland Revenue Department Act

1974. This Act connects the banks to the Inland Revenue Department.

- **Financial Transactions Reporting Act, 1996**

  The main aim of both FTRA (1996) and AMLCFTA (2009) is to help the banks to come out of fear and report the suspicious transactions to the police.

- **Information Technology Act, 2000**

  This is the primary law in India dealing with the cybercrime and electronic commerce.

- **Prevention of Money Laundering act, 2002**

  This Act is to protect either party in the banking sectors from being laundered.

- **Anti Money Laundering and Countering Financing of Terrorism Act, 2009.**

- **Personal Data Protection Bill, 2018.**

  The foremost purpose of this Act is the data privacy and the informational privacy for each and every citizen in our country. There are certain government schemes enacted for the privacy protection in banking transactions, one among them is the Banking Ombudsman Scheme. The core practice of this scheme is related to the collection and use of personal information of the customers in the banking sectors. There are definite ways for collecting the personal information such as in a written or oral form etc. It assures the banks with rights and it includes only the lawful and proper information. In the Judiciary, the Supreme Court held that the Right to Privacy under the Article 21 is a Fundamental Right. In *Puttaswamy v Union of India*[1], the Supreme Court held that the right to privacy is the intrinsic fundamental right mentioned in the Part III of the Constitution. The petition had been filed challenging the constitutional validity of the Indian Biometric Identity Scheme

[1] Writ petition (Civil) No 494 of 2012.

Aadhar. This judgement has over ruled the previous judgements of the Supreme Court in *Kharak Singh v State of U.P*[2] *and M.P. Sharma v Union of India.*[3]

REASONS BEHIND THE EMBITTERMENT:

- Carelessness on the part of either party may lead to the breach.

  As the author mentioned earlier, there are certain responsibilities on the part of the customers, so that they can be aware about the actual facts and prevent themselves from being cheated.

- No sufficient safeguards from the hackers

  With the increasing number of the technologies, the numbers of hackers are also increasing side by side which creates a fear in the minds of the people.

- Easy way to access the information

  As the author discussed above, there is no adequate advancement in our banking sectors which paves the way for the strangers to access the personal information of the banking customers.

- Sophisticated attack by the hackers

  Though the latest technological development has not yet reached the banking sector thoroughly, it enhances the route of the hackers to grasp the privacy of the customers in the banking transactions.

- Breach of Trust

  Since, with the advanced technologies, we all are fond of internet banking, which is easier than offline banking, as in our modern lifestyle, every individual might not feel comfortable to use offline banking transactions in their busy schedule. But as much as it is

[2] 1963 AIR 1295
[3] 1954 AIR 300

easier, there are equal level of difficulties and insecurities in online banking transactions. According to the recent census, the cyber crimes reported in India has increased 19 times over 10 years till 2014.

The five main threats to bank's cyber security are:

- Unencrypted data
- Malware
- Non secure 3rd party services
- Manipulated data
- Spoofing

SUGGESTIONS:

- Unawareness among the consumers

  India is a country with large number of population, though only 74% are literate and the remaining are illiterate. The knowledge about the banking and the related information is very low among our people, even the literate fails to answer about banking, so it is the duty of the people to improve their knowledge in banking sectors. At least once a year, the awareness programmes and workshops regarding the banking can be conducted by the concerned authority.

- No realization of the sensitive nature of the data

  The people fail to realise the nature of the data they are providing to the strangers, they should be provided awareness about the sensitive nature of the data.

- No proper consent

  People really don't know the value of their signature and consent. They fail to read out the rules and regulations completely but instead they put their signature in the places wherever it is required in the registration form.

- Faith in advertisements

This is one among the quickest ways to impress the customers so that they can be easily cheated by keeping faith in whatever things that has been delivered in the advertisements.

- No sufficient knowledge among the people

  As said earlier, there is less knowledge and awareness among the people regarding the privacy in banking transactions.

- No Adequate security

  It has been a question mark for the questions like: Whether there is adequate protection of the privacy in banking transactions? What is the present status for the privacy in banking transactions in India?

  The situation which exists today for the protection of the privacy in banking transactions is not perfect.

- Open banking

  Application Programming Interfaces (API). This has been in practice by the e-commerce giants like Amazon, e bay etc.

Some suggestions provided for the customers are:

- No fear to bring the problems to light
- Sufficient protection of the websites from the hackers
- Should not respond to any suspicious mails and messages
- Appointment of responsible members to monitor and protect the sensitive data

PRIVACY STATUS IN OTHER COUNTIRES:

As in our country, the sensitive information of the customers in their banking transactions are valued with much care and protected worldwide, through their laws and legislations. Many countries contribute a satisfactory level of shelter for the privacy of the people of their nation. For example the countries like U.S.A, Australia and Europe are paying a huge attention for the privacy of their people. Some of the events which stand as an evidence are: Wells Fargo paid $5.1

million to settle with the Securities and Exchange Commission (SEC) which is a measure taken by the US government to prevent abuses of consumer financial information but it hasn't been successful. Also in *Katz v United States*, the Supreme Court held that there should be an adequate and reasonable expectation of the privacy for an individual.

The U.S Congress has enacted several acts for the protection of the privacy of the customers, some of them are:

- Gramm Leach Bliley Act, 1999
- Financial Services Modernisation Act, 1999
- California Consumer Privacy Act, 2018

The European Union has also taken steps such as:

- General Data Protection Regulations (GDPR), May 25, 2018.
  Where the ultimate aim of these measures are to:
  1. Implement smart policies
  2. Educate and train employees
  3. Periodic audit of the security in Banks
  4. Possible Punitive actions immediately
  5. Laws regarding the banks

CONCLUSION:

Though India has taken several measures to protect the privacy in banking transactions, the awareness of progression proposed by the legislation has not reached all the levels of the Government. There should be a proper guide for the banks and financial institutions to inform about their procedures and directions in a right manner. There is a failure to provide administrative protection against different threats and also failure to make policies in tune with technological adjustments. Among all these drawbacks, the successful banks are still long lasting only in India. Though there may be a lot of criticisms over the banks, still they stand as a symbol of economic growth for our nation as it provides funds, loans for the people at the time of their needs and helps the public to get free from their financial crises.

"Banks are the ray of hope for the consumers"

Section-IV

Banking Laws and Reforms

"CRYPTO CURRENCIES - INDIAN LEGAL AND REGULATORY NEMESIS"

M. SIVARAMAN*
&
S. JEEVITHA**

ABSTRACT:

Crypto currencies have been in use for over a decade across the globe. But the regulation and adoption of practices regarding the use pose a great challenge to National and International Institutions. This paper examines the characteristics of crypto currencies with reference to legal practices, the challenges in treating them as property and where India stands in recognizing and regulating virtual currencies.

Introduction:

Bitcoins and other forms of crypto currencies known as virtual currencies have been in use for about a decade in several parts of the globe which initially emerged and survived without any regulation. Today there are attempts in some leading economies for executive and legislative regulation of such currencies. However, even in such jurisdictions, the legal character of crypto currency defies precise definition or delineation. No jurisdiction or Central Bank of any country recognizes it as a legal tender or lawful currency and as a consequence opinion is divided whether it is at least an asset, property or intellectual property or a commodity. Challenges not only remain in the regulation of such digital currencies, but also in relation to offences and crimes, fraud, terrorism and extortion, taxation, digital currency related contractual breaches, judicial intervention and enforcement, inheritance of such assets and a host of other issues.

Virtual Currencies: Creation and Characteristics:

Virtual currencies ("VCs") are created by successful completion and recording of transactions on block-chain which involves broadcasting the proposed transaction in the network, which is then further processed and verified by other participants in the network and

* Ph.D. Scholar, the Tamil Nadu Dr. Ambedkar Law University, Chennai.
** II year, B.A., LL.B (Hons.), VIT School of Law, Chennai.

if the transaction is valid, it is included in a subsequent block of transactions in the block-chain, which renders the process irreversible. Senders and recipients of VCs are identified by their public addresses corresponding to a set of digital keys, one being 'public' key and at least one 'private' key. Public and private keys are generated by a user's software without reference to the block-chain or the internet[1]. A transaction involving VCs is initiated by the sender who uses his digital signature with his private key to the public address of the recipient. The source of funds for this transaction is linked to one or more of his prior transactions which were already verified on the block-chain. The transaction is concluded when the private key of the sender in respect of his previous transaction is now vested on to the recipient, consummation of which is then broadcast to the blockchain network where it is processed and verified by other participants called the 'miners' and thereafter it becomes irreversible. The 'unspent transaction output' or 'UTXO' are locked to a specific owner recorded on the blockchain and recognized as units belonging to that specified owner by the said network, which designates multiple UTXOs that are recorded in various blocks of the chain. The balance UTXOs available to a user is calculated by a wallet application by scanning the blockchain and summing up all the UTXOs that are available to the accounts that the specific user is holding and controlling[2].The ownership rights in VCs rest in the ability to control the disposition of UTXOs that are recorded in the block-chain. This involves control through private keys so as to confer ownership to the VCs represented in that UTXO.

Legal Characteristics of Virtual Currencies& Global Practices:

The United States:

Judiciary in the United States have extended the notion and attributes of property law in an asset so as to exhibit three traits *viz*. an interest which is capable of precise definition, exclusive possession or control and a legitimate claim to exclusivity[3]. These standards were extended to electronic data initially to the internet domain names so as

[1] Andreas Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, O'Reilly Media, 2014.
[2] *Ibid*
[3] *Rasmussen*, 958 F.2d at 903, 1992 U.S. Court of Appeals for 9th Circuit.

to hold that they constitute a property[4] and subsequent decisions held that computer codes, confidential information regarding contracts with customers, business plans and products stored in electronic data form constitute property[5]. In order to attribute property interests to such electronic data, courts have evaluated whether such data has any independent economic value[6]. Applying the ratio of the decision in *Kremen* to virtual currencies, experts hold that an intangible property right vests in bitcoins under the California law[7]. Prof. Joshua Fairfield argues that the current property law needs to be reformed to better protect and promote ownership in digital assets such as virtual currencies[8], while Prof. Shawn Bayern highlights that bitcoin is a new kind of asset and that it will match parties' expectations if bitcoins are treated as intangible and movable personal property[9].

The United States Department of Treasury's Financial Crimes Enforcement Network requires every administrator or exchanger of VCs to register as a money services business[10] and US courts have also passed orders for seizure of bitcoins from an unregistered money services business and their forfeiture to the US Government concluding that such bitcoins were property subject to forfeiture under federal law[11] and for offences involving violation of money laundering laws also[12]. The Commodity Futures Trading Commission of the United States holds that virtual currencies fall within the ambit of commodities[13]. The U.S. Internal Revenue Service had issued a formal ruling stipulating that virtual currencies are treated as property for the purposes of federal tax and for transactions involving virtual

[4] *Kremen v. Cohen* 337 F.3d 1024, 1030 (9th Circuit, 2003)

[5] *Terarecon, Inc. v. Fovia, Inc*., No.C 05-4407 CW, 2006 WL 1867734, at 9 (N.D. Cal July 6, 2006)

[6] *See Dwyer v. American Express Co*., 273 Ill. App. 3d 742 (1995); *In re Jetblue Airways Corp. Privacy Litigation* 379 F. Supp. 2d 299, 327 (E.D. N.Y. 2005); *Thyroff v. Nationwide Mutual Insurance Co*., 8 N.Y. 3d 283, 292 (2007).

[7] Dax Hansen, J & Joshua L. Boehm, *Treatment of Bitcoin Under U.S. Property Law*, Perkinscoie.com/Blockchain, March 2017.

[8] Joshua Fairfield, *BitProperty*, 88 South California Law Review 805 (2015)

[9] Shawn Bayern, *Dynamic Common Law and Technological Change: The Classification of Bitcoin*, 71 Washington & Lee. Law Review Online 22 (2014)

[10] See Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001, Department of the Treasury, Financial Crimes Enforcement Network, March 18, 2013.

[11] *United States v. 50.44 Bitcoins*, No.CV ELH-15-3692, 2016 WL 3049166, (D.Md. May 31, 2016).

[12] *United States v. Ulbricht and Any and All Assets of Silk Road*, No.13 Civ. 6919 (JPO) (S.D.N.Y. Jan.27, 2014) Doc.22.

[13] Press Release: PR7231-15, *CFTC Orders Bitcoin Options Trading Platform Operator and its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps without Registering*, September 17, 2015.

currencies[14]. In relation to bankruptcy laws, the judiciary in United States treats VCs as properties[15]. New York was the first state in the United States to enact a BitLicence regulation which admits that crypto currency is to be regarded as property[16] and VCs are also regarded as digital assets for the purposes of trust and estate laws[17]. US courts also take a view that VCs can qualify as money as they can be purchased in exchange for legal tender[18]. Experts argue that the US prescriptions for block-chain accounting and ownership reporting in the current regulatory environment should be discouraged and instead it should be supported as a corporate voting instrument and as a possible corporate governance tool[19]. Efforts are also on to utilize crypto currencies as collateral securities within the existing framework under Article 9 of the Uniform Commercial Code of the United States for undertaking a secured transaction with some possible revisions and explanatory notes being added to Article 9 to provide clearer guidance[20].

***Europe*:**

In Germany, regulation for VCs exist in terms of the German Banking Act and the German Federal Financial Supervisory Agency has classified digital currencies. The German regime[21] on VCs envisage licensing requirement and its tax authorities classify VCs as 'economic asset' (*Wirtshaftsgut*) subjecting them to the German Income Tax; German criminal law is ill-equipped to classify theft involving VCs as an offence, unlike the Netherlands which holds theft of virtual money and virtual goods as offences[22]. Civil law in Germany is also deficient in treating VC and at best they are treated as IP rights under the German Copyright Act and seizure of VCs in Germany is also riddled with

[14] I.R.S. Notice 2014-21, 2014-16 I.R.B. 938 (April 14, 2014)
[15] *In re Hashfast Techs., LLC*, No.14-3011DM (Bankr. N.D. Cal. Feb. 22, 2016)
[16] N.Y. Comp. Code Rules & Regulations tit. 23, SS.200.1-200.22 ("23 NYCRR").
[17] Uniform Law Commission, Act Summary, Uniform Fiduciary Access to Digital Assets Act, Revised (2015), at p.2
[18] See *United States v. Faiella* 39 F. Supp. 3d 544, 545 (S.D.N.Y., 2014) and *SEC v. Shavers* No.4:13-CV 416, 2013 WL 4028182
[19] Fiammetta S. Piazza, *Bitcoin and the Blockchain as Possible Corporate Governance Tools: Strengths and Weaknesses*, Penn State Journal of Law & Intl. Affairs, Issue 2, Vol.2, 262.
[20] Timothy Bierer, *Hashing it out: Problems and Solutions Concerning Cryptocurrency Used as Article 9 Collateral*, Journal of Law, Technology & the Internet, Vol.7, 2016, 79.
[21] Franziska Boehm & Paulina Pesch, Bitcoin: *A First Legal Analysis – with reference to German and US-American Law*, as available in https://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_7.pdf last accessed on November 12, 2018
[22] Edwin Feldmann. Netherlands Teen Sentenced for Stealing Virtual Goods. http://www.pcworld.com/article/152673/virtual_theft.html , 2008 last accessed on November 12, 2018

challenges since they are not rights and it is felt that its current legal rules are not designed to handle the decentralized VCs. The United Kingdom regards VCs as an asset or 'private money' attracting capital gains tax, but exempts it from Value Added Tax, with its Government planning to bring the digital currency exchange firms within the scope of money laundering regime[23].

Japan recognizes them as 'real money'. Australia holds them as 'intangible property' subject to GST. Canada recognizes that VCs do not have legal tender characteristic and therefore fail the currency test, but would qualify as commodity for tax purposes[24]. Singapore refused to examine the characteristics of VCs, but, only chose to examine its effect and accordingly subjected it to tax under the Goods and Services Tax[25]. Brazil introduced Law No.12,865 in October 2013 to regulate payment arrangements, payment institutions and electronic currencies and the Brazilian Central Bank almost treats VCs as legal tender and thereby allows peer-to-peer mobile transfers[26]. China accords a special virtual commodity status to the VCs and prohibits its usage as currency or acceptance by banks or payment institutions[27]. Russia although initially prohibited VCs, has now softened its stand and has tolerated its usage till a legislation is brought in[28]. It is also opined that the Russian Federation ought to move towards a controlled financial and economic mechanism based on block-chain technology rather than the existing crypto currencies and smart contract systems[29]. The global practice is unanimous that no country has acknowledged VCs as either money or legal tender, but, several progressive jurisdictions have been quick to levy tax on them and also requiring registration and licensing of digital money exchanges.

---

[23] Hatim Hussain, *Reinventing Regulation: The Curious Case of Taxation of Cryptocurrencies in India*, 10 NUJS Law Review 3(2017)

[24] Jon Southrust, *Bitcoin is not Legal Tender, Says Canada Government Official*, Coindesk, January 17, 2014.

[25] Michael Lee, *Singapore Issues Tax Guidance on Bitcoins*, ZDNET, January 9, 2014.

[26] Becky Liggero, *Regulation of Bitcoin with David Gzesh*, Calvinayre.com (March 19, 2014) available at http://calvindayre.com/2014/03/19/business/bitcoin-regulations-david-gzesh-interview-bl-video/ as accessed on November 10, 2018

[27] Press Releases, *Monitoring the Use of Bitcoins*, News.Gov.HK (January 8, 2014) available at http://www.info.gov.hk/gia/general/201401/08/P201401080357.htm accessed on 14.11.2018.

[28] Evander Smart, *Russia Reconsidering Bitcoin Ban*, Cryptocoins News available at https://www.cryptocoinsnews.com/russia-reconsidering-bitcoin-ban-2015) accessed on November 10, 2018.

[29] Verzhevsky.P.A.,*Issues of Regulation of the Use of Crypto currency in the Russian Federation*, 2018, III Network AML/CFT Institute International Scientific and Research Conference "FinTech and RegTech: Possibilities, Threats and Risks in Financial Technologies, KnE p.267, Social Sciences.

Challenges in Treating Virtual Currencies as Property:

There are quite a few challenges mounted against VCs to deny property rights by arguing that the pseudo-anonymity character of the VCs pose a challenge in conferring a property right[30], the doctrine of property forms requiring a predetermined and closed set, it is argued that VCs would not fit into them[31], the multi-signature arrangements in VCs pose challenges to the 'control' aspect of property ownership and that there is a lack of traceability of VCs between owners across serial transactions[32]. Although VCs are not 'money' and 'legal tender', it is felt that governments will not surrender their privileges to regulate crypto currency issuers, exchanges, administrators and users. Experts caution that crypto currencies are not one-size-fits-all and therefore regulators should understand the unique technology underlying various types of crypto currencies and make a regulatory regime that acknowledges and regulates those differences according to the risks they pose[33]. As data is distributed among many ledgers, legal risk will remain and courts may have to interpret and hold that distributed ledger technology constitutes joint ventures with liability spread across all owners and operators of the systems serving as distributed ledgers and this legal approach should be focused by the regulators while seeking to support such digital currency systems[34].

How VCs are Misused?

There have been instances where VCs have been used for various unlawful and terrorist activities in several parts of the globe. VCs have been used for purchasing illegal goods *via* anonymous networks[35] and criminals have used VCs as a payment mode when blackmailing computer users, companies and even public authorities[36]. Digital

---

30 Ryan J. Straus & Mathew J. Cleary, *The Law of Bitcoin: The United States,* 187 (Jerry Brito, ed., iUniverse 2015)

31 Joshua Fairfield, *BitProperty*, 88 South California Law Review 805 (2015)

32 Patrick Murch, Presentation at Harvard University Berkman Centre for Internet & Society: *Property Law and the Blockchain* (October 20, 2015)

33 Edmund Mokhtarian and Alexander Lindgren, *Rise of the Crypto Hedge Fund: Operational Issues and Best Practices for an Emergent Investment Industry*, Stanford Journal of Law, Business & Finance, 2018, Vol.23:1, 112

34 Dirk A. Zetzsche, Ross PO. Buckley and Doughlas W. Arner, *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, [2017] UNSWLRS 52

35 See *United States v. Ulbricht and Any and All Assets of Silk Road*, No.13 Civ. 6919 (JPO) (S.D.N.Y. Jan.27, 2014) Doc.22.

36 *See* Ian Thompson, Cryptolocker Infects Cop PC: Massachusetts Plod fork out Bitcoin ransom http://www.theregister.co.uk/2013/11/21/police_pay_cryptolocker_crooks_to_get_their_computers_back/, 2013. *Also see*, Richard Meusers, Erpressersoftware: US-Polizistenzahlen Online-Kriminellen Bitcoin alsLosegeld.

currencies have been often used for money laundering as their traceability is complicated and their operation is highly decentralized and pseudo-anonymous as in the Cypriot capital in March 2013[37]. It is gathered that Islamic State in Syria (ISIS) had been using bitcoin for its fund-raising activities[38]. As VCs are a source of potential financial crimes, it is now exhorted that rather than having a cumbersome approach of enacting legislations by each nation, it would only be appropriate to have a globalized framework for regulating and overseeing digital currencies[39]. Although VCs may be faster and relatively fool proof payment and money transfer mechanism, there are glaring glitches in its operation due to its vulnerability to data security breaches, double spending and transaction malleability and miners' collusion. Although the blockchain creates immutable and unchangeable record of transactions which could be subject to forensic analysis of transaction history and behavior, the sheer open and voluminous nature of data held within the blockchain can be harnessed by law enforcement agencies only by more training and policing[40]. Despite there being no single coordinating centre, there already exists an international jurisdiction and state regulation of crypto currency activity will result in the implementation of legitimate and safe crypto currency relations[41]. Ownership of crypto currencies involves legal risk as fraud perpetrated through hacking in the absence of recourse against a third party such as a bank will render the holders of VCs fully exposed to loss[42].

Virtual Currencies in Indian Regime:

http://www.spiegel.de/netzwelt/web/cryptolocker-software-angriffi-us-polizei-zahlt-bitcoin-an-ransomware-a-93504815.html , 2013.

[37] Eric Garland, Cyprus bailout sends Bitcoin to more heights, http://www.transitionistas.com/2013/03/21/cyprus-bailout-sends-bitcoin-to-newheights/ , 2013 as accessed on 21.10.2018

[38] See ISIS Fundraising in US Via Bitcoin, January 30, 2015 available at http://www.rt.com/usa/227703-bitcoin-isis-us-fundraising/

[39] Tara Mandjee, *Bitcoin, its Legal Classification and its Regulatory Framework*, Journal of Business & Securities Law, Vol.15, Issue 2, 2016, p157.

[40] Gabrielle Patrick and Anurag Bana, IBA Legal Policy & Research Unit Legal Paper, *Rule of Law Versus Rule of Code: A Blockchain-Driven Legal World*, November 2017.

[41] Irina Cvetkova, *Crypto currencies Legal Regulation*, BRICS Law Journal, Vol. V(2018), Issue 2, 128

[42] Kelvin F.K. Low and Ernie Teo, *Legal Risks of Owning Crypto currencies*, (2017) Handbook of Digital Finance and Financial Inclusion, Vol.1, Crypto currency, FinTech, InsurTech, and Regulation, 225-248, Research Collection School of Law.

The Reserve Bank of India (RBI) initially cautioned the users of VCs, its holders and traders about the potential financial, operational, legal, customer protection and security related risks[43]. RBI followed it through with press releases on February 01, 2017 and December 05, 2017 cautioning all stakeholders on the various risks associated in dealing with such VCs. The RBI clarified that it was then examining the issues associated with its usage, holding and trading under the extant legal and regulatory framework of the country, including under the foreign exchange and payment systems laws and regulations. Finally, on April 6, 2018 it issued a statutory circular prohibiting all entities regulated by it not to deal in VCs or provide services for facilitating any person in dealing with or settling VCs[44]. At the same time, the RBI has acknowledged that block-chain could fight counterfeiting and bring huge revolution in the functioning of financial markets, collateral identification as well as payments system[45]. Security experts exhort that India should take urgent steps to regulate VCs by conferring it the status of asset, creation of a regulatory authority and exchanges for VCs, bringing the same under tax net, including capital gains tax, legislative support, training of the security agencies to investigate terror funding involving VCs, empowerment of judiciary to handle matters concerning VCs and cooperation with international agencies and countries[46].There does not exist any legislation governing VCs in India and therefore, its taxation aspect is out of question for the moment, but when a regulatory regime emerges for VCs in India, then probably the General Anti Avoidance Rules could enable the tax regulator in India to bring VCs within the ambit of the tax net. The White Paper released by Institute for Development and Research in Banking Technology, an arm of RBI, concludes that bitcoin technology has matured enough and there is sufficient awareness among the stakeholders making it an appropriate time for initiating suitable efforts towards digitizing the India Rupee through bitcoin technology[47] and it is also felt by several others that Indian Government should recognize VCs by self-regulatory

[43] Press Release dated December 23, 2013 of the RBI.

[44] RBI Circular No.RBI/2017-18/154 DBR.No.BP.BC.104/08.13.102/2017-18 dated April 6, 2018.

[45] Institute for Development and Research in Banking Technology, White Paper on Applications of Blockchain Technology to Banking, January 2017.

[46] TarandeepBains, *Bitcoin Digital Currency: A Portend for India's National Security*, CLAWS Journal, Winter 2015, pp.170-178

[47] Institute for Development and Research in Banking Technology, White Paper on Applications of Blockchain Technology to Banking, January 2017.

measures[48]. Although the Finance Minister had announced in his Budget speech on February 1, 2018 that VCs are not legal tender in India, he had acknowledged that industry has already recognized the blockchain technology and that the Government would try and explore the said technology in a digital economy[49].

Conclusion:

VCs may not be money or legal tenders in the current global scenario. However, there is no denying the fact that crypto currencies are faster, reliable and highly economical and cost effective money transfer systems. There is now emerging consensus on the legal nature and character of VCs which accord to them an asset or commodity or property status, subjecting them to property rights, including transfers, disposition through testamentary and non-testamentary modes, seizure and forfeiture by the state. They are also subject to levy of tax in several jurisdictions. Some jurisdictions have also expressly permitted the setting up of digital money exchanges through registration and licensing requirements. At the same time, various cybercrimes associated with VCs and the money laundering and terrorist fund raising through VCs pose challenges to law-enforcement agencies across the globe which have now started engaging the attention of regulators across the globe with realization dawning upon them that rather than prohibiting the digital currencies, it would make immense sense to regulate the same. India cannot afford to be left out of this technological innovative payment mechanism and asset characterization, but, as could be evident from the recent RBI paper and the Finance Minister's budget speech in February 2018, it appears that the Government is not only keen and open to the prospect of recognizing crypto currencies, but, is also engaged in delivering a highly calibrated response to its present risks, security, regulatory and tax related challenges. It is only a matter of time that RBI lifts the ban it had imposed and once the regulatory decks are cleared, VCs would come into the mainstream of payment settlement systems in our country.

[48] Nishith Desai Associates Report, *Bitcoins-A Global Perspective, Indian Legal and Tax Considerations*, April 2015.
[49] Budget Speech of Arun Jaitley, Finance Minister of India in the Parliament on February 1, 2018.

Legality of the "*Naming and Shaming*" Strategy Adopted by Banks Against Individual and Corporate Defaulters: Can the Bank Defame its Own Customers on the Ground of Wilful Defaults?

S. Mohammed Azaad*

"*Every life deserves a certain amount of dignity, no matter how poor or damaged the shell that carries it*".

- Mr. Rick Bragg, Pulitzer Prize Winning Writer[1]

ABSTRACT:

Banks borrow money from one customer (depositor) to lend it to another customer (borrower). The list of individual and corporate defaulters who are constantly missing payment deadlines is ever growing in India.

Thus, wilful debt defaults affect the Indian economy at large, as our nation is choking due to bad loans and non-performing assets (NPA) worth thousands of crores. The Reserve Bank of India (RBI) in its capacity as the Regulator and Supervisor of the Indian financial system has already put in place various measures with regard to the recovery process and categorisation of borrowers as non-cooperative or wilful vide its '*Master Circular on Wilful Defaulters*' dated 1st July 2015 (RBI/2015-16/100). Recently, on 29th September 2016, RBI issued another circular titled '*Publishing of Photographs of Wilful Defaulters*' (RBI/2016-17/71) which authorized the lending Banks to consider publication of the photographs of wilful defaulters.

The author submits that while defaulters have right to informational privacy implicitly guaranteed under Article 21 of the Indian Constitution, the same is not absolute and will be subject to

* Assistant Professor of Law, Tamil Nadu National Law University (TNNLU), Tiruchirappalli.

[1] Rick Bragg wrote this famous quote in his book, *All Over But the Shoutin*', New York: Pantheon Books, 1997. This quote is quoted with approval by *V. Chitambaresh, J.* in *P.R. Venu vs. The Assistant General Manager, State Bank of India & Another*, CDJ 2013 Ker HC 509 [*Venu's Case*].

reasonable restrictions imposed by the Banks. As right to privacy is not inviolable in nature, the next question that falls for consideration is whether the Bank with whom the customer has a fiduciary relationship is entitled to disclose or publicise the information in their possession, resulting in a breach of the duty of secrecy. In this regard, the author submits that while Banks have the right to recover their lawful dues by publishing the photos of defaulters, the same is subject to the confidentiality and secrecy obligations owed by a Bank (Lender or Creditor) towards its customer (Borrower or Debtor).

The research questions which will be addressed in the present paper are as follows:

- What amounts to a willful default according to RBI?
- Whether a person is a wilful defaulter or not can be left to the discretion of the lending banks?
- Do publication of the borrower's personal details by Banks is an acceptable method of recovery of outstanding dues authorised by law?
- Whether the Bankers right to adopt any lawful method for recovery of its dues, including the publication of the photograph of the defaulter is in direct conflict with the right to privacy and dignity of the borrower, which is implicitly guaranteed under Article 21 of the Indian Constitution?
- By publishing the photographs, are banks violating the banking secrecy and confidentiality laws?
- Should different standards be adopted by Banks for individuals and corporate defaulters while using the naming and shaming strategy?
- As debt default is a civil wrong and not being a criminal offence, can the rigour of embarrassment of the defaulters be so high?
- In the alternative, should wilful default be treated as a *per se* criminal offence?
- Whether the naming and shaming strategy unjustly defames the defaulters in the eyes of right thinking members of the general public?

I. Introduction

From time immemorial to the present day, almost every section of the population deals with banks and other similar financial institutions on a regular basis for various financial transactions such as depositing funds and valuables, taking out loans etc. As per Section 5(b) of the *Banking Regulation Act, 1949*[2] lending of funds is one of the primary functions of a bank. In the capacity of a Financial Intermediary, banks accept deposits of monies from the general public and consequently lend them to variety of borrowers in need ranging from individuals, small and mid-sized companies to big corporate moguls. In short, banks borrow money from one *customer (depositor)* to lend it to another *customer (borrower)*. The loans availed from the banks differs from customer to customer. It can be either secured or unsecured and the repayment cycle can be short term or long term. This lending function is of vital importance in a developing country like India, as the economic prosperity of the nation is directly proportional to the strong credit schemes of banking institutions.

Of late, we are seeing various news reports which say that borrowers are taking on crippling debts they can't repay anytime soon. Thus, the list of individual and corporate defaulters who are constantly missing payment deadlines is ever growing in India.[3] Now what happens if multitude of borrowers with large balances fail to repay their loans to their respective lenders? This will create serious sufferings not just for the borrowers who are subjected to serious financial penalties for defaults, but also for the innocent taxpaying citizens who are left with the financial burden of sharing the defaults by the unscrupulous borrowers.

In order to recover the loans, many Banks since the first part of 21st century have adopted a practice to publish the photographs and

---

[2] Section 5(b) of the Act reads as follows: "*Banking means the accepting, for the purpose of lending or investment, of deposits of money from the public, repayable on demand or otherwise, and withdrawal by cheque, draft, order or otherwise.*"

[3] See Anuradha Shukla, '*Centre Prepares List of 91 Defaulters to Prevent them from Fleeing Country*', The Indian Express, March 16, 2018, available at http://www.newindianexpress.com/nation/2018/mar/16/centre-prepares-list-of-91-defaulters-to-prevent-them-from-fleeing-country-1787874.html (last accessed: 5th December, 2018); See also '*Biggest Loan Defaulters in India*', Rediff, June 30, 2014, available at https://www.rediff.com/business/slide-show/slide-show-1-biggest-loan-defaulters-in-india/20131210.htm (last accessed: 5th December, 2018).

other personal details of loanees and their guarantors who have committed default in newspapers and on notice boards of bank branches as well as in the conspicuous spaces around their residence.[4] This '*naming and shaming*' strategy has been welcomed by many public sector lending banks as a significant weapon in their fight for recovering the lawful dues from perennial defaulters.[5]

As the RBI Circulars on wilful default are relatively new and are still undergoing changes, being a Lawyer and Academician myself, I would like to delve into the legality of laws relating to wilful default and the practice of naming and shaming the defaulters under Indian Banking laws by comparing the same with other jurisdictions. The primary aim is to question the naming and shaming practice, as it can affect the fundamental right to dignity and privacy of borrowers protected under Article 21 of the *Constitution of India, 1950* (hereinafter, '*Indian Constitution*'). Further, as this strategy is not strictly enforced in reality for big loan defaulters, when compared to small amount defaulters, I will check whether this differential treatment amounts to violation Articles 14 and 19 of the Indian Constitution.

II. Research Methodology and Research Questions

As the research study is primarily '*doctrinal*' in nature, my prime focus would be on theoretical data collection and analysis. Reviewing the existing judgments, legislative provisions, rules, regulations, circulars and policy documents of the RBI and Government of India relating to debt defaults and '*naming and shaming*' strategy as one of the methods for loan recovery constitutes my primary source of research. The materials which will be used for this study includes case laws, books, journals, articles and news reports. In addition, I have also consulted my advocate friends practicing in the DRT's and other debt

---

[4] ''*Name and Shame' Loan Defaulters: Banks Adopt New Tactic to Embarrass Debtors by Printing Their Names and Photos in Newspapers and Around Their Homes*', Mail Online India, July 10, 2013 [*Mail Online 2013*], available at https://www.dailymail.co.uk/indiahome/indianews/article-2359013/Name-shame-loan-defaulters-Banks-adopt-new-tactic-embarrass-debtors-printing-names-photos-newspapers-homes.html (last accessed: 5th December, 2018).

[5] *Ibid*; See also Press Trust of India (PTI), '*Banks to 'Name and Shame' Guarantors for Loan Defaulters*', The Economic Times, July 09, 2013, available at https://economictimes.indiatimes.com/industry/banking/finance/banking/banks-to-name-and-shame-guarantors-for-loan-defaulters/articleshow/20984705.cms (last accessed: 5th December, 2018).

recovery forums to understand the ground realities of the banking sector and to get a practical insight into the problems of loan defaults. The research questions which will be addressed in the present paper are as follows:

- What amounts to a willful default according to RBI?
- Whether a person is a wilful defaulter or not can be left to the discretionary decision of the lending banks?
- Is publication of the borrower's personal details by Banks an acceptable method of recovery of outstanding dues authorised by law?
- Whether the Bankers right to adopt any lawful method for recovery of its dues, including the publication of the photograph of the defaulter is in direct conflict with the right to privacy and dignity of the borrower, which is implicitly guaranteed under Article 21 of the Indian Constitution?
- By publishing the photographs, are banks violating the banking secrecy and confidentiality laws?
- Should different standards be adopted by Banks for individuals and corporate defaulters while using the naming and shaming strategy?

III. What amounts to 'Wilful Default'? Definition and Mechanism

Wilful debt defaults affect the Indian economy at large, as our nation is choking due to bad loans and non-performing assets (NPA) worth thousands of crores. As of 30th June 2018, wilful defaulters owe over Rs.15,300 crores to PNB and more than Rs.34,200 crores to SBI.[6] Further, according to the data presented in the Lok Sabha earlier this year, 9,501 wilful defaulters owed public sector banks

[6] Gireesh Chandra Prasad, '*Disclose Names and Action Taken Against Wilful Defaulters: CIC*', Livemint, August 29, 2018, available at https://www.livemint.com/Companies/0iQZ5PoGZAImCfph7e0EMM/Disclose-names-and-action-taken-against-wilful-defaulters-C.html (last accessed: 25thNovember, 2018).

approximately Rs.1.3 lakh crore.[7] The data showed that the number of defaulters rose by 14% and the amount they owed also rose by a staggering 70% from March 2016 to June 2018.[8]

RBI in its capacity as the regulator and supervisor of the Indian financial system has put in place various measures with regard to the recovery process and categorisation of borrowers as non-cooperative or wilful vide its 2015 '*Master Circular on Wilful Defaulters*'[9]. This circular has defined the term '*wilful default*'[10] in an expansive way. The mechanism[11] for deciding whether a person or a Company is a wilful defaulter or not is decided by an internal committee of the respective banks called as the '*Identification Committee*'. This committee is headed by an Executive Director or equivalent and consisting of two other senior officers of the rank of GM/DGM.[12]

With regard to the identification process, the circular declares that for a default to be categorised as wilful, "*it must be intentional, deliberate and calculated.*"[13] Further, the identification should be done by the Committee keeping in mind the overall track record of the borrowers and not on the basis of few isolated transactions or incidents.[14] The defaulter is also given an opportunity for a personal

---

[7] '*Just Four Banks Name and Shame Wilful Defaulters*', Financial Chronicle, November 12, 2018, available at http://www.mydigitalfc.com/deep-dive/just-four-banks-name-and-shame-wilful-defaulters (last accessed: 25thNovember, 2018).

[8] *Ibid.*

[9] *Master Circular on Wilful Defaulters*, RBI/2015-16/100, DBR.No.CID.BC.22/20.16.003/2015-16, dated July 01, 2015, available at https://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=9907 (last accessed: 25thNovember, 2018).

[10] *Ibid,* at para. 2.1.3 – "*Wilful Default: A 'wilful default' would be deemed to have occurred if any of the following events is noted:*

(a) The unit has defaulted in meeting its payment/repayment obligations to the lender even when it has the capacity to honour the said obligations.

(b) The unit has defaulted in meeting its payment/repayment obligations to the lender and has not utilised the finance from the lender for the specific purposes for which finance was availed of but has diverted the funds for other purposes.

(c) The unit has defaulted in meeting its payment/repayment obligations to the lender and has siphoned off the funds so that the funds have not been utilised for the specific purpose for which finance was availed of, nor are the funds available with the unit in the form of other assets.

(d) The unit has defaulted in meeting its payment/repayment obligations to the lender and has also disposed off or removed the movable fixed assets or immovable property given for the purpose of securing a term loan without the knowledge of the bank/lender.

[11] *Ibid,* at para. 3 which deals with *Mechanism for Identification of Wilful Defaulters*.

[12] *Ibid,* at para. 3(a).

[13] *Ibid,* at para. 2, p. 4.

[14] *Ibid.*

hearing, if the Committee feels such an opportunity is necessary.[15] The decision of the Identification Committeewill become final only after it is reviewed and confirmed by another committee called as the '*Review Committee*'[16]. Unlike the Identification Committee, this Committee consists of both internal as well as some independent members.

IV. Questioning the Discretional Authority of the Identification and Review Committees

The process of classifying defaulters as '*wilful*' and "*non – wilful*' was introduced by way of a scheme framed by RBI in April 1999.[17] The scheme was subsequently modified in 2002 and the latest position is reflected in the 2015 *Master Circular on Wilful Defaulters*. Now the issue is whether the categorisation of a person as a wilful defaulter can be solely left to the discretion of the lending banks. Even though this discretion is exercised via Identification and Review Committees, still there is a possibility that the Committees could be biased towards their own banks. Further, the opportunity for hearing given to a defaulter before the Identification Committee which purely consists of internal banking officials is not adequate, as the banks will be guided by their own self-interests rather than the interest of the customers.

It is pertinent to note that the entire process of marking someone as a wilful defaulter is fraught with subjectiveness. Moreover, it is not overseen or regulated by the RBI. As a consequence, the process is open to bias, manipulation and corruption, leading to instances of genuine wilful default not being classified and vice versa.[18] Thus, based on their own whims and fancies, the lending banks can adopt a pick and choose approach when it comes to labelling a borrower as a wilful defaulter and any error in such categorisation will lead to serious penalties.[19]

---

[15] *Ibid,* at para. 2(b).

[16] *Ibid,* at para. 3(c).

[17] *Ibid,* at para. 1.

[18] Garima Chitkara and Manisha Pande, '*RBI Defaulters List: Wilful or Non-Wilful? That is the Question*', News Laundry, April 26, 2016, available at https://www.newslaundry.com/2016/04/26/rbi-default-list-wilful-non-wilful-question (last accessed: 6th December, 2018).

[19] *Master Circular on Wilful Defaulters*, *supra* 9, at para. 2.5 which deals with '*Penal Measures*'.

As far as judicial review is concerned, if the State owned or a Nationalised bank has wrongly classified a person as a wilful defaulter, then the borrower can invoke the writ remedy before the High Courts or the Supreme Court. On the other hand, in the case of private banks, there is no scope for writ jurisdiction, as writ petitions can be filed only against the State or the instrumentalities of the State. Given the backlog of cases in India, even if the Company files a defamation suit or a complaint before the Consumer Forums against a private bank, it can still take ages to decide the matter and during the pendency of the suit, the defaulter will be irreparably harmed.

The unbridled discretion and excessive authority given by RBI to the banks is best summed up in an excellent piece by Professor Ajay Shah in the *Indian Express*, wherein he explains how the wilful defaulter classification is a gross violation of the rule of law:

> "*If a bank, P, determines that your default is wilful, then all other banks are forced to punish you. P gives you a bad name, and then all other banks, Q, are forced by RBI regulations to hang you. The formal processes of enforcement are missing and there are no adequate checks and balances. Non-state actors don't have the appropriate skills or incentives when it comes to justice. There is no mechanism for judicial review either.*"[20] (emphasis added)

V. Historical Perspectives – Tracing the Origin of Name and Shame Strategy

Recently, on 29th September 2016, RBI issued another circular titled '*Publishing of Photographs of Wilful Defaulters*'[21] which authorized the banks to consider publication of the photographs and other personal details of loanees who have committed default.Even before the 2016 Circular, the practice of humiliating the defaulters publicly to force them to cough up the loan amount existed since the last decade of the 20th century. Back in the 1990s, Citibank India, which is a

[20] Ajay Shah, '*How Not to Draft Regulation – RBI Rules on Wilful Default are a Throwback to the Age of Khap Panchayats',* The Indian Express, September 16, 2014, available at https://indianexpress.com/article/opinion/columns/how-not-to-draft-regulation/ (last accessed: 1st December, 2018).

[21]RBI/2016-17/71, DBR.CID. BC. No.17/20.16.003/2016-17), dated September 29, 2016, available at https://www.rbi.org.in/Scripts/BS_CircularIndexDisplay.aspx?Id=10619 (last accessed: 5th December, 2018).

subsidiary of the New York based multinational financial services corporation Citigroup became infamous for its habit of sending goondas and eunuchs to the homes and offices of loan and credit card defaulters with a view to publicly shame and threaten them.[22] Similarly, it was reported in 2013 that the Allahabad Bank has put out public notices in newspapers publishing not just the photograph of the borrower, but of the guarantors as well.[23] According to the bank officials, the rationale behind naming and shaming guarantors is to incite them into exerting moral and mental pressure on the defaulters.

Currently, the controversial practice of putting social pressure on defaulters by publishing their photos and contact details is followed by several prominent lending institutions like the SBI, UCO Bank, Indian Overseas Bank etc.[24]While Banks contend that they have the liberty to invent novel strategies like publishing photographs to recover their long standing dues, borrowers argue that publishing personal details in public platforms being a coercive, regressive and extra-legal method is a gross violation of their fundamental right to privacy and dignity enshrined under Article 21 of the Indian Constitution.

VI. Banks Right to Recover Dues vs. Borrowers Right to Privacy – Conflicting Judgements from High Courts

An analysis of the various judicial precedents around India shows that Madras,[25] Madhya Pradesh,[26] Chhattisgarh,[27] Gujarat[28] and Bombay High Courts[29] have encouraged the publication of photographs

[22]TamalBandyopadhyay, '*Pay Up or We'll Embarrass You*', Rediff, December 11, 2003, available at https://www.rediff.com/money/2003/dec/11banks.htm (last accessed: 10th December, 2018).

[23] See *Mail Online 2013, supra* 4.

[24] *Ibid.*

[25] *K.J. Doraisamy vs. The Assistant General Manager, State Bank of India*, 2006 (5) CTC 829 [*Doraisamy Case*]; *M/s.M.R. Motor Company and Others vs. The Federal Bank Ltd.,* W.P. No. 25737 of 2016, Judgement dated December 19, 2016; *M. Aruvi vs. Reserve Bank of India, Chennai & Another*, CDJ 2018 MHC 2762 [*Aruvi Case*]; *M/s. Mohan Breweries & Distilleries Ltd., Chennai vs. The Authorized Officer, State Bank of Mysore, Chennai*, CDJ 2018 MHC 3246.

[26] *Ku. Archana Chauhan vs. State Bank of India, Jabalpur*, AIR 2007 MP 45; *M/s. Revati Cements Private Ltd. vs. Allahabad Bank*, W.A. No. 549 of 2015, Judgement dated December 04, 2015; *Prakash Granite Industries vs. Punjab National Bank*, CDJ 2016 MPHC 209 [*Prakash Granite Case*].

[27] *Mohan Products Pvt. Ltd & Others vs. State Bank of India*, CDJ 2015 Ch HC 014.

[28] *Monal Dineshbhai Chokshi & Others vs. State Bank of India & Others*, CDJ 2015 GHC 380.

[29] *D.J. Exim (India) Pvt. Ltd. & Others vs. State Bank of India & Others*, CDJ 2014 BHC 1310 [*Exim Case*].

of defaulters as a method of loan recovery, whereas Kerala[30] and Calcutta High Courts[31] have frowned upon such practices. To understand the conflicting legal position, in the forthcoming pages, I will be summarising the crux of some of the landmark judgements delivered by the above Courts.

A. Madras High Court in Doraisamy Case[32]

It is one of the earliest judgements on the subject and which has been quoted regularly by other High Courts. Here the Madras High Court in the voice of V. Ramasubramanian J., famously held that "*if borrowers could find newer and newer methods to avoid repayment of the loans, then the banks are also entitled to invent novel methods to recover their dues.*"[33] The Court further held that right to privacy under Article 21 is not absolute in nature and from the Banks point of view, the duty to maintain secrecy is superseded by a larger public interest as well as by the bank's own interest to recover its lawful dues.[34] The Court also interpreted Section 8 of the *Right to Information (RTI) Act, 2005* and held that '*right to privacy*' of the defaulters fades out in front of '*right to information*' and '*larger public interest*'.[35] It is pertinent to note that this single judge order has been affirmed by a Division Bench of the Madras High Court in *W.A. No.1529 of 2006*[36] and is now considered as a settled legal position in the Madras circle.[37]

B. Madhya Pradesh High Court in Prakash Granite Case[38]

The Court categorically held that Rule 8 of the *Security Interest (Enforcement) Rules, 2002* (hereinafter, '*Security Interest Rules*') specifically authorised the banks to publish the names and addresses of the wilful defaulters. There is no legal bar either in the said rule or

---

[30] *Venu's Case*, *supra* 1.

[31] *Ujjal Kumar Das & Others vs. State Bank of India & Others*, CDJ 2013 Cal HC 074 [*Ujjal Case*]; *State Bank of India & Others vs. Ujjal Kumar Das & Another*, CDJ 2016 Cal HC 539 [*Ujjal Division Bench Case*]; *Metsil Exports Private Ltd. vs. Punjab National Bank*, CDJ 2016 Cal HC 550 [*Metsil Case*].

[32] *Supra* 25.

[33] *Ibid,* at para. 32.

[34] *Ibid,* at para. 29.

[35] *Ibid,* at para. 31.

[36] *Aruvi Case, supra* 25, at para. 5.

[37] *Ibid,* at para. 6. See also *M/s. Gain-N-Nature Food Products & Others vs. Galaxy Amaze Kingdom Ltd. & Others*, CDJ 2008 MHC 1717.

[38] *Supra* 26.

under any provisions of the *Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest (SARFAESI) Act, 2002* which expressly prohibits the bank from publication of photographs.[39]Therefore, the action of the banks in publishing the photographs cannot be held to be *ultravires*. However, the Court cautioned the banks to exercise their discretion judiciously and objectively, while classifying the borrowers as ordinary defaulters and wilful defaulters.[40]

C. Bombay High Court in Exim Case[41]

In this case, the Division Bench of the Bombay High Court took into consideration the differing judicial trends of the Calcutta (*Ujjal Case*) and Kerala High Courts (*Venu Case*) which heavily deprecated the practise of publishing the photograph of defaulters in newspapers. It finally held that these judgments are not binding, as the said decisions are challenged by the banks and the intra court appeal is pending before the concerned Division Bench. Even otherwise, the Bombay High Court held that we do not agree with the views expressed by the two learned Single Judges of the two High Courts[42] for the following reasons:

> "*A perusal of Rule 8 of the Security Interest Rules clearly indicates that the bank has the right to publish the name of the defaulters by giving their names and addresses. This serves two fold purposes. Firstly, the fact that these persons are wilful defaulters is made known to the public at large and secondly, it also tends to caution the prospective buyers who may be offered the property which is mortgaged by these defaulters with the bank. This being the primary objective for the publication of the notice, there would be no impediment in publication of photographs of wilful defaulters and particularly those defaulters who have committed various acts of misfeasance.*"[43] (emphasis added)

---

[39] *Ibid,* at para. 4.
[40] *Ibid,* at para. 5.
[41] *Supra* 29.
[42] *Ibid,* at para. 14.
[43] *Ibid,* at para. 11.

It is relevant to point out that this judgement was challenged by the Petitioners before the Supreme Court in the form of a Special Leave Petition. The same was summarily dismissed in 2014 and thereby confirming the validity of the Bombay High Court decision.[44] Subsequently, many Courts including the Delhi High Court[45] have followed this case as a binding precedent.

D. Calcutta High Court in Metsil Case[46]

In this case, per contra to the above mentioned judgements, Dipankar Datta J., of the Calcutta High Court ruled that there was no explicit provision for publishing photographs of defaulters under the *SARFAESI Act* or the *Security Interest Rules* framed there under. The Court followed the Division Bench judgement in *Ujjal Case,* wherein it was held that there is neither positive direction nor negative indication in the *SARFAESI Act or Rules* so far as publication of photographs is concerned.[47] Datta J., did not accept the divergent views from other Courts, as they have overlooked the principle of "*express mention of one thing impliedly excludes all other things*" found in the Latin legal maxim '*expressiouniusestexclusioalterius*'. He reasoned that by judicial fiat, the power to publish the personal details of borrowers cannot be conferred on the Bank officials, as the same is not expressly or even impliedly conferred by the parent legislation. His detailed line of reasoning is as follows:

> "*There being absolutely nothing in the parent enactment, i.e., 'the SARFAESI Act' conferring authority on the secured creditor to publish the photograph of a defaulting borrower, it would amount to stretching the Rules, i.e., 'the Security Interest Rules' to absurd limits to read into it the authority of a secured creditor to do so. It is well-known that a subordinate legislation supplements and cannot supplant the enactment to which it owes its origin. The Act being a self-contained code, it would be disastrous to read it and the Rules in a manner that would confer on authorized officers unfettered, unbridled and unchartered power while issuing sale notices. The rule*

[44] *D.J. Exim (India) Pvt. Ltd. & Others vs. State Bank of India, Mumbai & Others*, CDJ 2014 SC 617 [*Exim SC Case*].

[45] *K.V. Wall Mount Pvt. Ltd. & Others vs. State Bank of India*, W.P. (C) 8199/2013, Judgement dated December 08, 2014.

[46] *Supra* 31.

[47] *Ujjal Division Bench Case, supra* 31, at para. 24 on p. 8.

framing authority must have been conscious of the consequences, if an express power to publish photographs of defaulting borrowers were conferred on the authorized officers, and bearing the same in mind, it must be presumed to have chosen not to confer such power."[48] (emphasis added)

The Court found it unusual that the demand notice under Section 13(2) of the *SARFAESI Act*, apart from being served on the borrowers, was also published in two daily newspapers.[49] Therefore, the Court directed the Respondent bank to publish an apology in all the newspapers wherein it had published a demand notice under the *SARFAESI Act* with the photograph of the Petitioners.[50]

E. Kerala High Court in Venu Case[51]

In *Venu's Case*, a notice was issued by the lending banks instructing the borrower to make the payment due to the Bank, failing which the Bank expressed its intention to publish photograph of borrower with name and address. This was challenged and the High Court opined that there is nothing immoral in being unable to pay the loans availed of owing to the floundering of business or due to some other unavoidable reason which cannot enable the Bank to infringe the right to privacy of loanees.[52] It further opined that unless there exists a compelling public interest to publish photographs of the borrowers, it should not be resorted to in every default case, since routine procedure to publish photographs of every other defaulter may affect their right of privacy protected under Article 21 of the Indian Constitution.

Similar to *Venu's Case*, very recently, Dama Seshadri Naidu J., of the Kerala High Court held that demonstration by bank officials in front of defaulter's house violates his right to privacy. He inter alia observed as follows:

"*The bank can still have its legal methods of recovery. The Court does not come in the way. But its officials cannot conduct any sort of*

[48] *Metsil Case*, *supra* 31, at para. 12.
[49] *Ibid,* at para. 2.
[50] *Ibid,* at para. 37.
[51] *Supra* 1.
[52] *Ibid,* at para. 6.

'hallabol' demonstration in front of the Petitioner's house. Prima facie, it affects petitioners right to privacy, a most cherished fundamental, though unenumerated right".[53]

VII. Small Defaulters vs. Big Corporate Defaulters: Differential Treatment by Banks

It is ironical to note that while Banks are happy to embarrass individuals and small sized companies accused of defaulting small amounts, the Central Government and the RBI are still reluctant to disclose the names of top corporate defaulters of Rs.50 crores or more despite multiple directions and reminders from the Central Information Commission (CIC).[54] For instance, in *P.P. Kapoor vs. Reserve Bank of India*[55], an application was made enquiring about the details of the unpaid loans taken by the industrialists. The Applicant had also asked about the names of the top defaulters who have not repaid their loans to public sector banks. The RBI resisted the disclosure of information claiming exemptions under Sections 8(1)(a)[56] and 8(1)(e)[57] of the *Right to Information (RTI) Act, 2005* on the ground that disclosure would affect the economic interest of the country and that RBI in its capacity as a fiduciary has received information from the lending banks. The CIC found these arguments to be totally misconceived in facts and in law and held as follows:

"*I wish government and its instrumentalities would remember that all information held by them is owned by Citizens, who are sovereign. Further, it is often seen that banks and financial institutions continue to provide loans to industrialists despite their default in repayment of an earlier loan. Such practices have led citizens to believe that defaulters*

---

[53] Manu Sebastian, '*Demonstration by Bank Officials in Front of Defaulter's House Violates His Right to Privacy: Kerala HC*', Live Law, September 13, 2018, available at https://www.livelaw.in/demonstration-by-bank-officials-in-front-of-defaulters-house-violates-his-right-to-privacy-kerala-hc/ (last accessed: 5th December, 2018).

[54] *Shri Sandeep Singh Jadoun vs. CPIO, DGEAT*, Orders of the CIC dated August 21, 2018 and November 16, 2018 [*Sandeep Singh Case*], available at https://indiankanoon.org/doc/3802339/ (last accessed: 8th December, 2018).

[55] Order of the IC dated November 15, 2011 [*Kapoor Case*]. See also *Jayantilal N. Mistry vs. Reserve Bank of India*, Order of the Information Commissioner (IC) dated November 1, 2011.

[56] Section 8(1)(a) of the Act reads as follows: "*information, disclosure of which would prejudicially affect the sovereignty and integrity of India, the security, strategic, scientific or economic interests of the State, relation with foreign State or lead to incitement of an offence.*"

[57] Section 8(1)(e) of the Act reads as follows: "*information available to a person in his fiduciary relationship, unless the competent authority is satisfied that the larger public interest warrants the disclosure of such information.*"

can get away and play fraud on public funds. There is no doubt that information regarding top industrialists who have defaulted in repayment of loans must be brought to the citizens' knowledge; there is certainly a larger public interest that would be served on disclosure of the same. In fact, information about industrialists who are loan defaulters of the country may put pressure on such persons to pay their dues."[58] (emphasis added)

It is noteworthy to mention that the Supreme Court as early as in December 2015 itself has upheld various orders of the CIC and Information Commissioners (IC) and directed the RBI to disclose information about wilful defaulters and the actions taken against them to the public.[59] Even as the RBI shows reluctance to make the names of wilful defaulters public, four state owned banks (IDBI,[60] Bank of Baroda,[61] Syndicate Bank[62] and Punjab National Bank[63]) have already uploaded the lists of wilful defaulters along with the amounts they owe on their websites.

It is pertinent to note that many big corporate fraudsters and scamsters have left India since 2010[64] and the latest to join the list is Mr. Nirav Modi in the *PNB Fraud Case*.[65] While there are some news reports claiming that the Finance Ministry has written a letter to the lending institutions directing them to "*formulate a policy with the approval of their board of directors which clearly set out the criteria for*

---

[58] *Kapoor Case, supra* 55, at p. 4.

[59] *Reserve Bank of India & Others vs. Jayantilal N. Mistry & Others*, CDJ 2015 SC 979 [*Jayantilal Case*].

[60] *List of Wilful Defaulters Above Rs.25 Lakhs – Suit Filed and Non Suit Filed Category as on 10.12.2018*, available at https://www.idbi.com/pdf/DisplayofWDlist-16May2018.xlsx (last accessed: 5th December, 2018).

[61] *List of Wilful Defaulter Accounts as on 28.02.2017*, available at https://www.bankofbaroda.com/download/Final-Willful-defaulters-28022017.pdf (last accessed: 5th December, 2018).

[62] *List of Wilful Defaulters of Rs.25 Lakhs and Above as on 30.06.2018*, available at https://www.syndicatebank.in/downloads/WILFUL_DEFAULTERS_25_LAKH.pdf (last accessed: 5th December, 2018).

[63] *List of Wilful Defaulters with Outstanding Rs. 25 Lakhs and Above as on 30.11.2018*, available at https://www.pnbindia.in/wilful-defaulters.html (last accessed: 5th December, 2018).

[64] Noor Mohammad, '*After Nirav Modi, a Look-Back at High Profile Indian Businessmen Who Have Skipped Town*', The Wire, February 19, 2018, available at https://thewire.in/business/nirav-modi-look-back-high-profile-indian-businessmen-skipped-town (last accessed: 10th December, 2018).

[65] '*Indian Billionaire Jeweller Nirav Modi Flees to UK, Claiming Political Asylum – Financial Times*', Reuters, June 11, 2018, available at https://uk.reuters.com/article/uk-britain-india-nirav-modi/indian-billionaire-jeweller-nirav-modi-flees-to-uk-claiming-political-asylum-ft-idUKKBN1J610N (last accessed: 10th December, 2018).

publication of photographs of wilful defaulters"[66], yet in reality no concrete action has been taken by the Central Government. This is evidenced by the latest November 2018 order of the CIC in *Sandeep Singh Case,*[67] wherein the CIC sent a show cause notice to the RBI and PMO, asking why maximum penalty should not be imposed on them for failing to provide information related to wilful defaulters to the public as directed by the Apex Court in *Jayantilal's Case* (cited *supra*).[68] The CIC also made a scathing remark that the RBI Governor and his colleagues were dishonouring the SC verdict.[69] Instead of obeying the order, RBI filed a petition in the Bombay High Court challenging the CIC's order. Currently, the Court has granted interim stay on the Order until the next hearing which is scheduled on 19th April, 2019.[70]

There is a difference between a borrower who had taken loan for basic needs like home loan, educational loan etc. and other big corporate borrowers who avail loan for lofty business reasons. The name and shame approach is rigorously applied only for loans given to individuals as well as small and medium enterprises, while the big corporate moguls are escaping the clutches of law, as the Central Government and Central Bank reckons that disclosing their names in public would hamper the companies' health, if they are in genuine difficulty and may accentuate the failure of business rather than nursing it back to health.[71] The CIC noted that while small amount defaulters like farmers and early stage entrepreneurs are defamed in public, big corporate defaulters who are renowned for disreputable business practices are bestowed with high concessions and privileges in the name of one time settlements, interest waivers etc., and all along

[66] Press Trust of India (PTI), '*Govt Asks Banks to 'Name and Shame' Wilful Defaulters*', The Times of India, March 13, 2018, available at https://timesofindia.indiatimes.com/business/india-business/govt-asks-banks-to-name-and-shame-wilful-defaulters/articleshow/63288019.cms (last accessed: 5th December, 2018).

[67] *Supra* 54.

[68] *Ibid,* at para. 56.

[69] *Ibid.*

[70] NitishKashyap, '*Bombay HC Grants Interim Stay on CIC's Order Directing RBI to Disclose Wilful Defaulters' List*', Live Law, December 16, 2018, available at https://www.livelaw.in/bombay-hc-grants-interim-stay-on-cics-order-directing-rbi-to-disclose-wilful-defaulters-list/ (last accessed: 10th December, 2018).

[71] TamalBandyopadhyay, '*It's Time to Name and Shame Defaulters*', Rediff, December 04, 2018, available at https://www.rediff.com/business/report/its-time-to-name-and-shame-defaulters/20181204.htm (last accessed: 10th December, 2018).

their names are hidden from exposure to secure their reputation.[72]This fallacious and reprehensible approach by banks is fundamentally flawed, as it amounts to arbitrary differential treatment violative of Articles 14 and 19 of the Indian Constitution. In any event, there is an argument that high profile corporate borrowers are too thick skinned to be shamed, even if their names are made public which to a certain extent is true.

VIII. Conclusion:

To recover the money from the defaulters, Banks contemplate various legal actions such as through the *Debt Recovery Tribunals* or through the recently enacted *Insolvency and Bankruptcy Code (IBC), 2016*. The RBI's policy to name and shame the defaulters is one of the methods to plug the various loopholes in lending laws of India. Banks believe that the threat of public condemnation acts as a deterrent for borrowers from becoming potential defaulters. However, Banks should keep in mind that for a civil and economic wrong like defaults, the rigour of embarrassment cannot be so high as to be equated with a criminal offence. If the Banks misuse the '*name and shame*' strategy, it will simply outrage and infringe the basic rights attached with human dignity.

With regard to the '*right to privacy and secrecy vs. right to innovative loan recovery strategies*' debate, apart from the *Exim Case*, there is no authoritative ruling by the Supreme Court to resolve the divergent views of the various High Courts. Accordingly, there is no uniformity as to whether Banks can continue to publish personal details of delinquent borrowers in India. I submit that that while defaulters have right to informational privacy and dignity implicitly guaranteed under Article 21 of the Indian Constitution, the same is not absolute and will be subject to reasonable restrictions imposed by the Banks.

As right to privacy is not inviolable in nature, the next question that falls for consideration is whether the Bank with whom the customer has a fiduciary relationship is entitled to disclose or publicise

[72] *Sandeep Singh Case, supra* 54, at para. 8.

the information in their possession, resulting in a breach of the duty of secrecy. In this regard, the I submit that while Banks have the right to recover their lawful dues by publishing the photos of defaulters, the same is subject to the confidentiality and secrecy obligations owed by a Bank (Lender or Creditor) towards its customer (Borrower or Debtor). The law relating to maintaining confidentiality and secrecy of customers' accounts was laid down in the famous English case of *Tournier vs. National Provincial and Union Bank of England.*[73] This law is followed in India also and the exceptions to the *Tourniers Rule* are as follows:

> "*(a) where the law mandates the disclosure, (b) where there is a duty to disclose to the general public, (c) where the interest of the bank warrants disclosure, (d) where the disclosure is made after getting the express or implied consent of the customer and (e) where the custom or practice mandates for such disclosure.*" (emphasis added)

Thus, the duty of the Bank to maintain secrecy can be superseded by the Bank's own legitimate interest of recovering the debt amount from the borrowers. Of course, there will be genuine instances where the borrowers are not able to pay because of external circumstances that have impacted their business. Hence, adequate caution and due discretion should be exercised by Banks before putting the names of defaulters in public domain. The banking institutions should spare the innocent individuals and serious entrepreneurs, but shouldn't allow the rogues to use the shield of privacy, reputation or confidentiality.

[73] 1924 1 K.B. 461.

NON-PERFORMING ASSETS AND MEASURES TO REDUCE IT

Gadde Shareesh*

ABSTRACT:

When the advances and loans made by the bank or financial institution turn out to be unproductive and non-yielding they take the form of Non-Performing Assets (NPAs). The most important ingredient which measures the health of the banking industry is the size of Non-Performing Assets (NPAs). Non-Performing assets have direct influence on the financial efficiency of banks i.e. their profitability.

Indian Banking System is at the centre of Indian economy which fulfils the basic requirement of the Priority Sector as well as Non – priority Sector by providing Advance/Loan facilities. The Operational, Financial, Social, Political and Economic inconsistency existing in the system creates difficulties to repay the loan amount sanctioned up to some extent, which subsequently becomes Non Performing Assets for the Banks and Financial Institutions. Non-Performing Assets (NPAs) are one of the major distresses for banks in India.

From the regulator's viewpoint, there are four steps to the management/evaluation of NPAs, namely assessment, provisioning, recovery and prevention of fresh NPAs.

There were numerous Acts to govern NPA concerns and matters such as the Sick Industrial Companies (special provision) Act, 1985 ("SICA"), SARFAESI Act, 2002, the Recovery of Debts due to Banks and financial institutions Act, 1993 ("RDDBFI Act"), Companies Act, 1956 as well as Companies Act, 2013. But these regulations have not yielded satisfactory results which leads to introduction of Insolvency and Bankruptcy Code 2016.

This paper aims to first explain the NPAs & NPAs Level in the banking sector in India and then examine the causes for raising NPAs. In the closing part of the article, measures which banks can take to minimize their NPAs have been recommended.

* Mr. Gadde Shareesh, Chartered Accountant Student (CA Final).

Steps like Preventive and Curative management are necessary to prevent assets from becoming Non-Performing Assets. Government and RBI are required to take such steps to recover and reduce NPA's. It is better to avoid NPAs at the primary stage of credit consideration by putting in place of thorough and appropriate credit appraisal and monitoring mechanisms.

Introduction:

The growth of the economy depends upon the efficiency and stability of the banking sector. The most important factor which measures the health of the banking industry is the size of NPAs. Non-Performing assets have direct impact on the financial performance of banks i.e. their profitability.

Concept of NPA has been introduced by Narasimham Committee on Financial System Reforms in 1991. The problem of NPAs is linked with the lending procedure of banks as these are an unavoidable burden on the banks. Based on borrower promise bank will provide amount and earn income over a period of time. If borrower is unable to pay loan availed from bank then bank has to lose both the income and capital. Banks today are facing the difficulty of Non- performing assets which pose risk to the survival of all the banks.

Definition of NPA's:

An asset, including a leased asset, becomes non-performing when it ceases to generate income for the bank. A **Non-Performing Asset (NPA)** was defined as a credit facility in respect of which the interest and/or instalment of principal has remained **past due** for a specified period of time. The specified period was reduced in a phased manner as under:

With effect from March, 1993 – Four Quarters

With effect from March, 1994 – Three Quarters

With effect from March, 1995 – Two Quarters

With effect from March, 2001 – 180 days

With effect from March, 2004 – 90 days

With a view to moving towards international best practices and to ensure greater transparency, it has been decided to adopt the 90 days overdue norms for identification of NPAs from the year ending March 31, 2004. Accordingly, with effect from March 31, 2004 a non-performing asset (NPA) shall be a loan or an advance where:-

- Interest and/or instalment of principal remains overdue for a period of more than 90 days in respect of term loan.
- The account remains out of order for a period of more than 90 days, in respect of an overdraft/ cash credit (OD/CC).
- The bills remain overdue for a period of more than 90 days in the case of bills purchased and discounted.
- Interest and/or instalment of principal remains overdue for **two harvest seasons** for a period not exceeding two half years in the case of an advance granted for agricultural purposes and
- Any amount to be received remains overdue for a period of more than 90 days in respect of other accounts.

Various committees, financial institutions and legislations interpreted NPAs in different ways to define NPA in respective terms.

Definition as per Narasimham Committee

The problem of NPA was first brought into focus by the Narasimham Committee on financial system (1991), set up with the initiation of liberalization process in the country. The Committee placed emphasis on identifying problem loans of banks and making provisions for such loan and so instituted proper definition of NPAs. Apart from identification of bad assets the Committee also suggested some ways to deal with them. Further, Narasimham Committee clearly defined that an asset may be treated as Non-performing Asset (NPA), if interest or installments of principal or both remain unpaid for a period of more than 180 days. However, with effect from March 2004, default status is given to a borrower account if dues not paid for a period of 90 days.

Definition according to Prudential Norms

According to the prudential norms, an asset, including a leased asset, becomes non-performing when it ceases to generate income for the bank. A non-performing asset was defined as a credit facility in respect of which interest remained past due for a period of four quarters in the year ending March 31, 1993, three quarters during the year ending March 31, 1994 and two quarters during the year ending March 1995 and onwards

Definition as per RBI Guidelines

RBI guidelines defined that NPAs consist of substandard assets, doubtful assets and loan assets. Any asset usually turns as NPA when it fails to yield income during a certain period. As a result, doubtful assets find their way from substandard assets after 18 months in Indian context (against 12 months under the international norms of NPAs.) If it is found irrecoverable, then it migrates to loss assets category.

Definition according to SARFAESI Act, 2002

The Securitization and Reconstruction of Financial Assets and Enforcement of Security Interest (SARFAESI) Act, 2002 defined Non-Performing Assets as an asset or account of a borrower, which has been classified by a bank or financial institution as substandard, doubtful or loss assets in accordance with the direction or guidelines relating to asset classification issued by the RBI.

NPA Classification:

The NPAs have been classified under four categories:

- **Standard Assets:** A standard asset is a performing asset. Standard assets generate continuous income and repayments as and when they fall due. Such assets carry a normal risk and are not NPAs in the real sense.
- **Sub-standard Assets:** All those assets which are considered as non-performing for a period of 12 months.

- **Doubtful Assets:** Those assets which are considered as non-performing for period of more than 12 months.
- **Loss Assets:** All those assets which cannot be recovered.

Provisioning of NPA's:

Based on the asset classification banks are required to make provision against the NPAs at 100% for loss assets; 100% percent of the unsecured portion plus 20% to 50 % of the secured portion, depending on the period for which the account has remained in doubtful category; and 10% etc. Banks have constituted Recovery Cells, Recovery Branches, and NPA Management Departments and fix recovery targets. Policies evolved and steps taken in this regard are critically examined during the annual on-site inspection of banks. The off-site returns also provide RBI an insight in to the quality of credit portfolio and quarterly intervals.

Introduction of prudential norms on income recognition, asset classification and provisioning during 1992 - 93 and other steps initiated apart from bringing in transparency in the loan portfolio of the banking industry have significantly contributed towards improvement of the pre-sanction appraisal and post-sanction supervision which is reflected in lowering of the levels of fresh accretion of non-performing advances of banks after 1992

Types of NPA's

NPAs are broadly divided into two types:

a) **GROSS NPA:**

Gross NPAs are the sum total of all loan assets that are classified as NPAs as per RBI guidelines as on Balance Sheet date. Gross NPA reflects the quality of the loans made by banks. It consists of all the non-standard assets like as sub-standard, doubtful and loss assets. It can be calculated with the help of following ratio:

Gross NPAs Ratio = [Gross NPAs/Gross Advances] X 100

b) **NET NPA**

Net NPAs are those type of NPAs in which the bank has deducted the provision regarding NPAs. Net NPA shows the actual burden of banks. Since in India, bank balance sheets contain a huge amount of NPAs and the process of recovery and write off of loans is very time consuming, the provisions the banks have to make against the NPAs according to the central bank guidelines, are quite significant. That is why the difference between gross and net NPA is quite high. It can be calculated with the help of following ratio:

Net NPAs = [Gross NPAs – Provisions/Gross Advances – Provisions] X 100

Factors contributing for rise in NPA's

There are many reasons as to why a loan goes bad. They are as follows:

a) External Factors

- ***Ineffective Recovery Tribunal:*** The Govt. has set of numbers of recovery tribunals, which works for recovery of loans and advances. Due to their negligence and ineffectiveness in their work the bank suffers the consequence of non-recovery, thereby reducing their profitability and liquidity.
- ***Will-full Defaults:*** There are borrowers who are able to pay back loans but are intentionally withdrawing it. These groups of people should be identified and proper measures should be taken in order to get back the money extended to them as advances and loans.
- ***Natural Calamities:*** This is the major factor, which is creating alarming rise in NPAs of the PSBs. Every now and then India is hit by major natural calamities thus making the borrowers unable to pay back their loans. Thus the bank has to make large amount of provisions in order to compensate those loans, hence end up the fiscal with a reduced profit. Mainly our farmers depend on rain fall for cropping. Due to irregularities of rain fall the farmers are not able to achieve the production level thus they are not repaying the loans.

- ***Industrial Sickness:*** Improper project handling, ineffective management, lack of adequate resources, lack of advance technology, day to day change Government policies etc. give birth to industrial sickness. Hence the banks that finance those industries ultimately end up with a low recovery of their loans reducing their profitability and liquidity.

- ***Lack of Demand:*** Entrepreneurs in India are not able to foresee their product demand and start production which ultimately piles up their product thus making them unable to pay back the money they borrow to operate these activities. The banks recover the amount by selling of their assets, which covers a minimum label. Thus the banks record the non-recovered part as NPAs and have to make provision for it.

- ***Change in Government Policies:*** With every new Government, banking sector gets new policies for its operation. Thus it has to cope with the changing principles and policies for the regulation of the rising of NPAs. The fallout of handloom sector is continuing as most of the weavers Co-operative societies have defaulted largely due to withdrawal of state patronage. The rehabilitation plan worked out by the Central Government to revive the handloom sector has not yet been implemented. So the overdues due to the handloom sectors are becoming NPAs.

b) Internal Factors:

- ***Defective Lending process:*** There are three cardinal principles of bank lending that have been followed by the commercial banks since long. (i) Principles of safety, (ii) Principle of liquidity and (iii) Principles of profitability .By safety it means that the borrower is in a position to repay the loan both principal and interest. The repayment of loan depends upon the borrowers- a) Capacity to pay, b) Willingness to pay.

- ***Inappropriate Technology:*** Due to inappropriate technology and management information system, market driven decisions on real time basis cannot be taken. Proper Management Information System (MIS) and financial accounting system is not implemented

in the banks, which leads to poor credit collection, thus it leads to increase in NPAs. All the branches of the bank should be computerized.

- ***Improper SWOT Analysis:*** The improper strength, weakness, opportunity and threat analysis is another reason for rise in NPAs. While providing unsecured advances the banks depend more on the honesty, integrity, and financial soundness and credit worthiness of the borrower.

    - Banks should consider the borrowers own capital investment.
    - It should collect credit information of the borrowers from bankers; enquiry from market/segment of trade, industry, business and from external credit rating agencies
    - **Analyse the Financial Statements:** True picture of business will be revealed on analysis of Profit and loss Account and Balance Sheet.
    - **Purpose of the loan:** When bankers give loan, it should analyze the purpose of the loan. To ensure safety and liquidity, banks should grant loan for productive purpose only. Bank should analyze the profitability, viability, long term acceptability of the project while financing.

- ***Poor Credit Appraisal System:*** Poor credit appraisal is another factor for the rise in NPAs. Due to poor credit appraisal the bank gives advances to those who are not able to repay it back. They should use good credit appraisal to decrease the NPAs.

- ***Managerial Deficiencies:*** The banker should always select the borrower very carefully and should take tangible assets as security to safe guard its interests. When accepting securities banks should consider the – (1) Marketability (2) Acceptability (3) Safety (4) Transferability. The banker should follow the principle of diversification of risk based on the popular maxim "do not keep all the eggs in one basket"; it means that the banker should not grant advances to a few big farms only or to concentrate them in few industries or in a few cities. If a new big customer meets

misfortune or certain traders or industries affected adversely, the overall position of the bank will be affected.

- ***Absence of Regular Industrial Visits:*** The irregularities in spot visit also increases the NPAs. Irregular visits by bank officials to the customer point decreases the collection of interest and principle on the loan. The NPAs due to wilful defaulters can be collected by regular visits.
- ***Re-loaning Process:*** Non remittance of recoveries to higher financing agencies and reloaning of the same have already affected the smooth operation of the credit cycle. Due to re loaning to the defaulters by CCBs and PACs, the NPAs of OSCB is increasing day by day.

The origin of the burgeoning problem of NPAs lies in the quality of managing credit risk by the banks concerned. What is needed is having adequate preventive measures in place namely, fixing pre-sanctioning appraisal responsibility and having an effective post-disbursement supervision. Banks concerned should continuously monitor loans to identify accounts that have potential to become non-performing

Impact of NPAs on banks

NPAs directly affect the profitability of the banks. Below mentioned are the ways through which banks profitability is affected:

- **Liquidity position:** NPAs affects the liquidity position of the banks, thereby creating a Mis-match between assets and liability and force the banks to raise resources at high cost.
- **Undermine bank's image:** High level of NPAs shadows the image of banks both in domestic and global markets. This ultimately leads to lower profitability.
- **Effect on funding:** Increasing level of NPAs in banks results in scarcity of funds in the Indian capital market as there will be only few banking institutions who will lend money.

- **Higher cost of capital:** It shall result in increasing the cost of capital as banks will now have to keep aside more funds for the smooth working of its operations.
- **High risk:** NPAs will affect the risk-bearing capacity of the banks.
- **Effect on income:** NPAs will reduce the net interest income of the banks as interest is not charged to these accounts.
- **Declining productivity:** It will also cost in terms of time, money and manpower which will ultimately results in declining profitability, since the staff is primarily engaged with preparing papers for filing law cases to recover principal amount and interest rather than devoting time for planning mobilization of funds.
- **Effect on ROI and profitability:** It reduces the earning capacity of the assets thereby negatively affect the ROI. All NPAs need to be prudentially provided for which shall have a direct impact on the profitability of the banks.
- **Ultimate burden on society:** It will ultimately affect the consumers who now will have to fetch out more money for paying higher interest

Level of NPA in Banking Sector[1]

The gross NPA ratio for Public Sector Banks (PSBs) as a category is 14.6% in the financial year (FY) 2017-18, as per Reserve Bank of India (RBI) data. Bank-wise details of gross NPAs as on March 2018, and operating profit, provision done for financial year 2017-18 has been specified below:

SL.No	Bank	Operating Profit for F.Y 2017-18	Gross NPA ratio (%)	Provision For NPA in 2017-18
1	Andhra Bank	5,361	17.1%	8,774
2	Canara Bank	9,548	11.8%	13,770

[1] RBI Global operations data March 2018.

3	State Bank of India	59,511	10.9%	66,058
4	Oriental Bank of Commerce	3,703	17.6%	9,575
5	Vijaya Bank	3,098	6.3%	2,371
6	UCO Bank	1,334	24.6%	5,771
7	Punjab National Bank	10,294	18.4%	22,577
8	Indian Overseas Bank	3,629	25.3%	9,929
9	Indian Bank	5,001	7.4%	3,742
10	Corporation Bank	3,950	17.4%	8,004
11	Indian Overseas Bank	3,629	25.3%	9,929
12	United Bank of India	1,025	24.1%	2,479
13	Syndicate Bank	3,864	11.5%	7,087
14	Punjab & Sind Bank	1,145	11.2%	1,889

As a result of transparent recognition of stressed assets as NPAs, the aggregate Gross NPAs of PSBs (as per Reserve Bank of India (RBI) data on global operations), have increased from Rs.2,79,016 crore, as on 31.3.2015 to Rs.8,95,601 crore, as on 31.3.2018 (provisional data).

Measures:

A number of measures have been taken to recover loan amount from NPAs, and wilful defaulters. As a result, PSBs recovered an amount of Rs.1,58,259 crore, during the financial years 2015-16 to 2017-18. To avoid recurrence and for stringent recovery, the Insolvency and Bankruptcy Code, 2016 (IBC) has been enacted to create a Unified Framework for resolving insolvency and bankruptcy matters. The Banking Regulation Act, 1949 was amended, to provide for authorisation to RBI to issue directions to banks to tackle the insolvency resolution process under IBC. Under this, by adopting a

creditor-in-saddle approach, with the interim resolution professional taking over management of affairs of Corporate Debtor at the outset, the incentive to resort to abuse of the legal system was taken away. This coupled with debarment of wilful defaulters and persons associated with NPA accounts from the resolution process, has effected a fundamental change in the creditor-debtor relationship. Further, as per RBI's directions, cases have been filed under IBC in the National Company Law Tribunal (NCLT) in respect of 39 large defaulters, amounting to about Rs.2.69 lakh crore funded exposure (as of December 2017). In addition, recapitalisation of PSBs, announced and initiated by the Government, has enabled upfront provisioning, easing apprehensions in actively pursuing resolution.

Further, the **Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002** (SARFAESI Act) has been amended for faster recovery with provision for three months imprisonment in case the borrower does not provide asset details and for the lender to get possession of mortgaged property within 30 days. Also, six new Debts Recovery Tribunal have been established to expedite recovery.

In addition, under the PSB Reforms Agenda announced by the Government, PSBs have committed to strengthen recovery mechanism by setting-up Stressed Asset Management Verticals for focussed recovery, clean and effective post-sanction follow-up on large-value accounts by tying up with Agencies for Specialised Monitoring for loans of Rs.250 crore and above, and strict segregation of pre- and post-sanction roles for enhanced accountability.

To reduce incidence of default on account of and to effect recovery from wilful defaulters, as per RBI's instructions, wilful defaulters are not sanctioned any additional facilities by banks or financial institutions, their unit is debarred from floating new ventures for five years, and lenders may initiate criminal proceedings against them, wherever necessary. As per data reported by PSBs, as on 31.3.2018, 2,323 FIRs have been registered against wilful defaulters, 8,835 suits have been filed for recovery from them, and action has been initiated under the SARFAESI in respect of 7,300 cases of wilful defaulters.

Securities and Exchange Board of India (SEBI) Regulations have been amended to debar wilful defaulters and companies with wilful defaulters as promoters/directors from accessing capital markets to raise funds. Further, the Insolvency and Bankruptcy Code has been amended to debar wilful defaulters from participating in the insolvency resolution process.

Steps to the management/evaluation of NPAs:

From a RBI study conducted in 1999, which though confined to only big borrower accounts, it was inferred that the factors, responsible for creation of NPAs, external to the bank are more predominant than those attributable to the bank. In such a case the role of the Government and the RBI assumes critical importance in ensuring a credit market climate wherein the legal system is more responsive and there is sufficient deterrence to wilful defaulters and those who take recourse to litigation for just buying time. Once such environment is created the NPAs levels for different banks will depend to a large extent on their own policies, systems, and judgements and perhaps will gravitate to reasonably low levels reflecting the time credit market risks. From the regulator's perspective, there are four steps to the management of NPAs, namely:

Assessment,

Provisioning,

Recovery and

Prevention of fresh NPAs.

The recent initiatives in management of NPAs relate in greater measure to the third and fourth aspect, viz., recovery and prevention aspect although norms relating to the first and second aspects have been progressively tightened to bring them at par with international best practices.

Approaches to Control NPA's

It is proved beyond doubt that NPAs in bank ought to be kept at the lowest level. Two pronged approaches namely:-

Preventive Management:

a) **Credit Assessment and Risk Management Mechanism:** A lasting solution to the problem of NPAs can be achieved only with proper credit assessment and risk management mechanism. The documentation of credit policy and credit audit immediately after the sanction is necessary to upgrade the quality of credit appraisal in banks. In a situation of liquidity overhang the enthusiasm of the banking system is to increase lending with compromise on asset quality, raising concern about adverse selection and potential danger of addition to the NPAs stock. It is necessary that the banking system is equipped with prudential norms to minimize if not completely avoid the problem of credit risk.

b) **Organisational Restructuring:** With regard to internal factors leading to NPAs the onus for containing the same rest with the bank themselves. These will necessitate organizational restructuring, improvement in the managerial efficiency, skill up gradation for proper assessment of credit worthiness and a change in the attitude of the banks towards legal action, which is traditionally viewed as a measure of the last resort.

c) **Reduce Dependence on Interest:** The Indian banks are largely depending upon lending and investments. The banks in the developed countries do not depend upon this income whereas 86 percent of income of Indian banks are accounted from interest and the rest of the income is fee based. The banker can earn sufficient net margin by investing in safer securities though not at high rate of interest. It facilitates for limiting of high level of NPAs gradually. It is possible that average yield on loans and advances net default provisions and services costs do not exceed the average yield on safety securities because of the absence of risk and service cost.

d) **Potential and Borderline NPAs under Check:** The potential and borderline accounts require quick diagnosis and remedial measures so that they do not step into NPAs categories. The auditors of the banking companies must monitor all outstanding

accounts in respect of accounts enjoying credit limits beyond cut – off points, so that new sub-standard assets can be kept under check.

Curative Management:

The curative measures are designed to maximize recoveries so that banks funds locked up in NPAs are released for recycling. The Central government and RBI have taken steps for arresting incidence of fresh NPAs and creating legal and regulatory environment to facilitate the recovery of existing NPAs of banks. It follows once NPA has occurred, one must come out of it or it should be managed in the most efficient manner. Legal ways and means are there to overcome and manage NPAs.

Legal Measures like ARC's and DRT has been established. Non legal Measures like Reminder System, Visit to Borrower's Business Premise/Residence, Recovery Camps, Rephrasing Unpaid Loan Instalments and Rehabilitation of Sick Units. One such possibility is recovering the dues through compromise.

Effective credit monitoring, as per the laid down procedures, gives enough clues to identify the sickness of a unit as it is surfacing. However, the misery is that there is always a wide gap between expectations and reality. Yet, becoming an NPA. The branch has to necessarily be alert to pick up sickness signals at the very initial stage and launch corrective measures so as to arrest fresh accretions to the NPAs.

CONCLUSION:

The government is taking many steps to reduce the problem of NPAs but banks should also have to be more proactive to adopt a structured NPAs policy to prevent the non-performing assets and should follow stringent measures for its recovery.

References:

1. Kumar, T.S. (2008), "An Imperative for the Development of Financial Markets", The Financial Analyst, Hyderabad, Vol.XIV, Issue 10, October Issue, pp. 89-91.

2. Borbora R.R., “Management of Non-Performing Assets (NPAs) in the Urban Cooperative Banks (UCBs)”, Reserve Bank of India, 2007.

3. Ahmed J.U., “Am Empirical Estimation of Loan Recovery and Asset Quality of Commercial Banks”. The NEHU Journal, Vol.8 (1), 2010.

4. KaminiRai, “Study on Performance of NPAs of Indian Commercial Banks” Asian Journal of Research Banking and Finance, Volume 2, Issue 12, December 2012.

DIGITAL INDIA – A NEED FOR A COMPREHENSIVE LEGAL CODE

Bagavathy Vennimalai*

ABSTRACT:

"India is the world's largest experiment in digitalisation."

- B. Santhanam, Saint-Gobain India

In the midst of technology becoming more accessible and affordable in India, electronic banking has emerged in the Indian Banking system. Digital banking has played a unique role in strengthening the banking sector and improving service quality in commercial banks. With the increased use of digital payments, customers need to be protected from unauthorised banking transactions. The increase in the number of persons using internet and the misuse of technology in the cyberspace has instigated cyber crimes at the domestic as well as in the international level. This paper revolves around cyber frauds in the banking sector which is one of the largely unregulated grey areas in India. The author has felt the need to examine the digital banking in India as it has witnessed different forms of cybercrimes like ATM frauds, Phishing, identity theft, Denial of Service and the hacking of debit cards and bank accounts that has become common. The laws on digital payments being awfully vague, the author tries to analyse the existing legal mechanism in India to prevent banking frauds in internet banking. Scrutinizing the Information Technology Act, the author identifies the lacunae in the existing legislative framework. Comprehending the fact that in a bid to step up customer protection in the era of digitisation, the Reserve Bank of India has set up a goal to curb cyber crimes in the banking sector, the author indicates the need for a robust regime for the prevention of cyber attacks in the banking sector.

* 4th year student, B.Com L.L.B. (Hons.) School of Excellence in Law, the Tamil Nadu Dr.Ambedkar Law University, Chennai.

I. Introduction

With the extensive use of technology particularly internet by users, banking is becoming more dependent on technology. On the recommendation of the Committee on Financial System (Narasimham Committee) 1991-1998, information and technology in banking sector was used. Until mid-1990s, banking sector in most parts of the world was simple and reliable; however since the advent of technology, the banking sector saw a paradigm shift in the phenomenon.[1] Banks in order to enhance their customer base introduced many platforms through which transactions could be done without much effort.[2] These technologies enabled the customer to access their bank finances 24*7 and year around through, ATMs and Online banking procedures. Unfortunately, with this the cyber-crimes related to banks are also increasing stupendously.[3] Inadequate technology implementation can also induce strategic risk in terms of strategic decision making based on inaccurate data/information.[4] Banking sector has witnessed expansion of its services and strives to provide better customer facility through technology but cyber-crime remains an issue. Information which is available online is highly susceptible to be attacked by cyber criminals.[5]

The tendency of cyber security attacks aimed at financial sector is much high than any other sector. This causes a tremendous loss of money to the customer and bank, declines bank's reputation and decreases the trust that users place in a bank. The Banking industry has been exposed to a large number of cyber-attacks on their data privacy and security such as frauds with online payments, ATM machines, electronic cards, net banking transactions, etc.[6] The average number of attacks aimed at financial services institutions is four times

---

[1] JALESHGARI, R., '*Document trading online*', INFORMATION WEEK, 755: 136 (1999).

[2] VRANCIANU, M., & POPA, L. A., '*Considerations Regarding the Security and Protection of E-Banking Services Consumers Interests*', THE AMFITEATRU ECONOMIC JOURNAL, 1228: 388-403 (2010).

[3] ZAHOOR, ZARKA, '*Challenges in Privacy and Security in Banking Sector and Related Countermeasures*', INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS (0975 – 8887) Vol.144 – No.3 (June, 2016) p.24.
See: G.GOPALAKRISHNA, *Report of the Working Group on information security, electronic banking, technology risk management, and tackling cyber frauds*, RBI, Mumbai, Maharashtra, (Jan. 2011) <https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=6366>

[4] RBI Guidelines on Information Security, Electronic Banking, Technology Risk management and Cyber Frauds, 2012.

[5] SONI RR AND SONI NEENA, *An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks*, Vol. 2(7), 22-27, July (2013), RESEARCH JOURNAL OF MANAGEMENT SCIENCES.

[6] ZARKA, '*Challenges in Privacy and Security in Banking Sector and Related Countermeasures*', INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS (0975 – 8887) Vol.144 – No.3 (June, 2016) p.27.

than that of companies in other industries according to a new report from Websense Security Labs.[7] The main reason behind these intrusions is to gain confidential data or steal money from banks.

As consumers continue to advance towards digitization, pressure mounts on the IT infrastructures of financial institutions. They must race to provide innovative digital services while also ensuring that robust information security standards are in place to protect and benefit both consumers and the bank itself. In turn, banks are facing an unprecedented challenge of cyber security breaches. McKinsey predicts the cost of implementing and managing cyber security infrastructure to increase by 40% by 2025.[8] According to the Indian Emergency Response Team (CERT-In) approximately 28,000 cyber security incidents were reported in June 2017. The Reserve Bank of India (RBI), has provided guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds. The guideline is intended to facilitate proactive response and management of cyber incidents.

II. Existing Framework to Protect Digital Banking

1. I.T. Legislation in India

As the misuse of technology was increasing at a very high rate, a strict statutory law to regulate the criminal activities in the cyber world was the need of the hour. To control these fraudulent practices Indian parliament enacted the **Information Technology Act, 2000**[9] on 17th October 2000 which deals with the laws in the field e-commerce, e-governance, and e-banking as well as fines and punishments to be imposed to control cybercrimes. The I.T. Act, 2000 and the I.T. Amendment Act, 2008 were enforced with reference to banking and financial sector transactions.[10] Government of India enacted its Information Technology Act, 2000 with its objectives stated in Act itself

---

[7] DR. MANISHA M.MORE, MEENAKSHI P.JADHAV AND DR. K.M.NALAWADE, *'Online Banking and Cyber Attacks: The current Scenario'*, INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND SOFTWARE ENGINEERING, vol. 5, no. 12, pp. 743-749, 2015 ISSN: 2277 128X.

[8] *The Future of Bank Risk Management*, MCKINSEY & COMPANY, (July 2016).

[9] Hereinafter referred to as 'I.T. Act, 2000'

[10] VINAYA, CHATURVEDI, *"Cyber Crime: Technological Blight in Digital Banking in India"*, IOSR JOURNAL OF BUSINESS AND MANAGEMENT (IOSR-JBM,) pp. 60.

"to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

The previous Act was the subject of certain debates, reviews and few criticisms. The need for an amendment was felt for the I.T. Act from the year 2003-04. Major industrial bodies were consulted and advisory groups were formed to suggest recommendations for the need of Information Technology (Amendment) Act, 2008.[11] The I.T. (Amendment) Act, 2008 considers main issues like data privacy, information security, defining cybercrime, making digital signature technology neutral, defining reasonable security practices to be followed by corporate, redefining the role of intermediaries, recognizing the role of Indian Computer Emergency Response Team, inclusion of some additional cyber crimes like child pornography and cyber terrorism, authorizing an Inspector to investigate cyber offences,[12] etc.

2. RBI Regulating Cyber Crimes in India:

Keeping in mind the dramatic swell in online economic crimes, India's central bank issued a comprehensive circular[13] to all banks in India urging them to implement a cyber security framework. It prescribes the ideal approach for banks on taking concrete measures to combat cybercrime, fraudulent activities online and thereby retain customer confidence, reduce financial losses and ensure business continuity.[14] RBI's circular covered several notable suggestions, ranging from arrangements for continuous surveillance, creation of a cyber

[11] Hereinafter referred to as 'I.T. (Amendment) Act, 2008'.

[12] VINAYA, CHATURVEDI, "*Cyber Crime: Technological Blight in Digital Banking in India*", IOSR JOURNAL OF BUSINESS AND MANAGEMENT (IOSR-JBM,) p. 59.

[13] *Cyber Security Framework in Banks*, RBI CIRCULAR DBS.CO/CSITE/BC.11/33.01.001/2015-16, dated June 2, 2016.

[14] *'How can RBI's latest guidelines help Indian banks combat cybercrime?'*, CLARI5, CUSTOMERXPS, <https://www.clari5.com/multichannel-banking-technology/can-rbis-latest-guidelines-help-indian-banks-combat-cybercrime/> (last visited on 16/12/2018).

security policy that is distinct from the broader IT policy and an immediate assessment of gaps in preparedness to be reported to the regulator. To diminish future risks and fortify safety mechanisms, institutions using global payment services should conduct a complete security review of their IT infrastructure. Lastly, a proactive forensic analysis of all the systems may be beneficial to ascertain if there has already been a breach or compromise.[15]

With the emerging threat landscape, where organised cybercrime and cyber warfare are gaining prominence, the RBI is working towards ensuring continuous protection against the changing contours of cyber security threat. The central bank's agenda for 2018-19 include enhanced level of protection against cyber risks to ensure continuous protection against the changing contours of internet based security threats. The RBI's report said the 2018-19 agenda include taking effective steps to "further enhance" the levels of protection against cyber risks. [16]

III. Cyber Crimes in Banking Sector

Banks are exposed to a number of cyber security attacks. RBI identifies Phishing, Cross site scripting, Vishing, Cyber Squatting, Bot networks, E-mail related crimes, Malware, SMS spoofing, Denial of service attacks, Pharming, Insider threats as the emerging information security attacks on banks.[17]

1. Phishing

Phishing, one of the most common cyber frauds, is an attack in which an attempt is made to obtain sensitive information of user by pretending to be a reliable body in an electronic communication. Phishing is typically carried out by email spoofing or instant messaging

---

[15] AMIT JAJU, *'Countering emerging cyber threats in the banking sector'*, LIVE MINT, <https://www.livemint.com/Opinion/9YDMKwqI8tRnLx7NSEJGcN/Countering-emerging-cyber-threats-in-the-banking-sector.html> (last visited on 17/12/2018).

[16] *RBI working on measures to further beef up cyber security in FY19*, THE ECONOMIC TIMES, Dated Sep. 03, 2018<//economictimes.indiatimes.com/articleshow/65656064.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst> (last visited on 17/12/2018).

[17] G.GOPALAKRISHNA, '*Report of the Working Group on information security, electronic banking, technology risk management, and tackling cyber frauds'*, RBI, Mumbai, Maharashtra, (Jan. 2011) <https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=6366>

in which users are asked to click on a link usually for securing their accounts. These tools include Botnets, Phishing Kits, Abuse of Domain Name Service (DNS), Technical Deceit, Session Hijacking and Specialized Malware.[18] A phishing incident was reported in Hyderabad,[19] in which the phishing email said that RBI had launched a new security system and asked users to enter their online bank credentials including card numbers and the secret three digit CVV number, among others. RBI has cautioned people that it has not launched any such software as soon as it came to know about it.

In the case of *Umashankar Sivasubramanian* v. *ICICI Bank*,[20] the petitioner used to receive monthly bank account statement under the email ID of the bank, one day received a mail asking for his personal details, which he provided, after which his account was debited with Rs.5 lakhs. Upon complaint, the bank said that it was a phishing mail against which he approached the adjudicating officer. In this case, the bank was held liable according to Section 43 and Section 85 of the IT Act, 2000, as it failed to establish due diligence and providing adequate checks and safeguards to prevent unauthorized access into the customer's account. In *National Association of Software and Services Companies* v. *Ajay Sood*[21], a reasoned order approving a settlement agreement between the plaintiff and the defendants in a case which dealt with the issue of 'phishing', with a decree of ` 16 lakhs was passed in favour of the plaintiffs.

2. Cross Site Scripting

Cross-site scripting (XSS) is a kind of cyber security vulnerability usually found in web applications and they allow code injections by malicious web users into the web pages that are viewed by other users.[22] A cross-site scripting vulnerability can be exploited by attackers to bypass access controls. Their impact ranges from a petty

[18] JINGGUO WANG, '*Research Article Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email*', IEEE TRANSACTIONS ON PROFESSIONAL COMMUNICATION, Vol. 55, Issue: 4, (Dec. 2012) <https://ieeexplore.ieee.org/document/6289402> (last accessed on 16/12/2018)

[19] R.P.KAUR, '*Statistics Of Cyber Crime In India: An Overview*', INTERNATIONAL JOURNAL OF ENGINEERING AND COMPUTER SCIENCE, vol.2, no. 8, pp. 2555-2559 (2013).

[20] *Umashankar Sivasubramanian v. ICICI Bank*, Petition No. 2462 of 2008 (Judgment Dated 12th April 2010)

[21] *National Association of Software and Services Companies* v. *Ajay Sood,* 119 (2005) DLT 596, 2005 (30) PTC 437 (Del).

[22] ZAHOOR, ZARKA, '*Challenges in Privacy and Security in Banking Sector and Related Countermeasures*', INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS (0975 – 8887) Vol.144 – No.3 (June, 2016).

nuisance to a significant security risk, depending on the sensitivity of the data that is handled by the vulnerable site and the nature of any security mitigation implemented by the site's owner.

3. Vishing

Vishing (voice + phishing) is a cyber-attack in which social engineering and Voice over IP (VoIP) are used to access the private and financial information from the public for getting financial reward.[23] Vishing is an illegal practice where an attacker calls a user and pretends to be from a bank in which the user has an account. In an attack in 2014, customers of a midsize bank received SMS text messages which claimed their debit card was deactivated and asked users to provide the card and PIN numbers to reactivate it.[24]

4. Cyber Squatting

Cyber-squatting is a process in which a famous domain name is registered and then it is sold for a fortune. Cyber Squatters register domain names which are similar to popular service providers' domains so as to attract their users and benefit from it. Some countries have specific laws against cyber-squatting that are beyond the normal rules of trademark law. For example, the United States has the U.S. Anti cyber - squatting Consumer Protection Act (ACPA) of 1999 which provides protection against cyber squatting for individuals and also owners of distinctive trademarked names. The Washington Post reported in 2007 that Dell filed a lawsuit against Belgium Domains, Capitol Domains, and Domain Doorman for cyber-squatting and typo-squatting and dell financial services.com was one of the domains that was cited.[25]

5. Bot Networks (Botnet)

Bots are programs that infect a system to provide remote command and control access via a variety of protocols, such as HTTP,

---

[23] G.GOPALAKRISHNA, *'Report of the Working Group on information security, electronic banking, technology risk management, and tackling cyber frauds'*, RBI, Mumbai, Maharashtra, (Jan. 2011) <https://rbi.org.in/ scripts/ NotificationUser.aspx?Mode=0&Id=6366>

[24] JOHN LA COUR, '*Vishing campaign steals card data from customers of dozens of banks'*, (April 29, 2014) <http://blog.phishlabs.com/vishing-campaignsteals-card-data-from-customers-of-dozens-of-banks>

[25] HEMANT BHADANA, *'Legal Position of Cyber squatting in India'*, <https://blog.ipleaders.in/laws-tackling-cyber-squatters-cyber-squatting/> (last accessed on 02/10/2018).

instant messaging, and peer-to-peer protocols. Several of bots under common control, commonly referred to as a "Botnet". Computers, get associated with botnets when unaware users download malware such as a "Trojan Horse" which is sent as an e-mail attachment. The systems that are infected are termed as "zombies".

6. Malware

Malware is a maliciously crafted software program that accesses and alters the computer system without the consent of the user or owner. Malware can heavily influence the confidentiality, integrity and availability of the banking system. Malwares have the capability to compromise the information in the banking systems and may lead to a loss of millions to the bank. Malwares can target both the user's system and the bank itself.

7. Denial of Service (DOS) Attack

A DOS is an attack in which an user or an organisation is prevented from accessing a resource online. Actually the targeted system is flooded with incoming messages which causes it to shut down and thus the system is unavailable to its users. DOS attacks can cost the bank a great deal of time, money and customers and can also destroy programming and files in affected computer systems.

8. SMS Spoofing

It is a relatively new technology in which a user receives a SMS message on phone which appears to be coming from a legitimate bank. In this SMS the originating mobile number (Sender ID) is replaced by alphanumeric text. Here a user may be fooled to give his/her online credentials and his/her money may be at risk of theft.

9. TCP/IP Spoofing

In IP spoofing, illegal access is attempted on a system by sending an email message to a victim that appears to come from a trusted machine by spoofing the machines' IP address. However using IP spoofing, the attacker's data packet appears to come from legitimate IP address (internal network) and thus firewall is unable to intercept it. The main goal here is to obtain root access to the victim's server (here

the banking system), allowing a backdoor entry path into the targeted systems.[26]

10. Pharming

It is also called farming or DNS poisoning. In this attack whenever a user tries to access a website, he/she will be redirected to a fake site. Pharming can be done in two possible ways: one is by changing host's files on a victim's computer and the other way is by exploiting vulnerability in DNS server software. In January 2008, a drive-by pharming incident was reported by Symantec that was directed against a Mexican bank and in which the DNS settings on a customer's home router were altered after receipt of an e-mail message that appeared to be from a legitimate Spanish-language greeting-card company.[27]

11. Insider Threats

With the increase in the use of information technology by banks, there is a high security risk to bank's data by insiders or employees of banks who can disclose, modify or access the information illegally. Also unintentional errors by employees can have devastating results. Robust security processes must be used by banks to mitigate such threats.

12. Attacks on OTP

OTP (one Time Password) is a two factor authentication method in which a password is created whenever the users attempts authentication and the password is disposed of after use. Attacks that can be launched on accounts that are OTP protected are as follows: [28]

- ***Man-in-the-middle attack (MITM):*** Here the transmission paths of data are accessed and information is snatched in the middle of transactions.

[26] MOHD KHAIRUL AHMAD, RAYVIEANA VERA ROSALIM, LEAU YU BENG AND TAN SOO FUN, '*Security issues on Banking Systems*', INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGIES, vol. 1, no.4, pp. 268-272, 2010 ISSN: 0975-9646.

[27] ELLEN MESSMER, '*First case of drive-by pharming identified in the wild*' (Jan 22, 2008) http://www.networkworld.com/article/2282527/lanwan/first-case-of--drive-by pharming--identified-in-the wild.html (accessed on 19/09/2018).

[28] CHANGSOK YOO, BYUNG-TAK KANG AND HUY KANG KIM, '*Case study of the vulnerability of OTP implemented in internet banking systems of South Korea*', Multimed Tools Appl ,vol. 74, pp. 3289–3303, 2015.

• ***Man-in-the-Browser attack (MITB):*** Here malicious code exists in the web browser and it induces users to enter credentials and other important information into a fake form.

• ***Man-in-the-PC attack (MITPC):*** MITPC exploits the weaknesses in the hardware environment or operating system to steal OTP.

13. Hacking

Hacking is an unauthorized access made by a person to cracking the systems or an attempt to bypass the security mechanisms, by hacking the banking sites or accounts of the customers. The Hacking is not defined in the amended IT Act, 2000.[29] But under Section 43A read with section 66 of Information Technology (Amendment) Act, 2008 and under Section 379 & 406 of Indian Penal Code, 1860, a hacker can be punished.

IV. Challenges Faced by the Banking Sector in the Digital Era

The dependence on technology is so much that the banking sector cannot be thought of without the use of technology. But technology has also brought a whole set of challenges to be dealt with which include external threats leading to cyber frauds,[30] higher impact due to intentional or unintentional acts of internal employees, new social engineering techniques used to gain confidential credentials.[31] Digital banking can be a nightmare because buyers then are at the mercy of a bewildering maze of computer servers, bots and infuriating call centres.

1. Liability for e-wallet transactions

It is pertinent to note that there are virtually no options to retrieve the money that has been lost in the cyber space. While the RBI has banking rules for reconciling failed ATM transactions within seven working days after a customer complaint, there are no such guidelines

[29] *Types of Cyber Crimes & Cyber Law in India*, <http://www.csiindia.org/c/document_library/get_ file?uuid=047c826d-171c-49dc-b71b-4b434c5919b6>, (Last visited 30/4/2015)

[30] Alaganandam, H., Mittal, P., Singh, A., & Fleizach, C. 2007. Cybercriminal Activity.

[31] DR. MANISHA M.MORE, MEENAKSHI P.JADHAV AND DR. K.M.NALAWADE, *'Online Banking and Cyber Attacks: The current Scenario'*, INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND SOFTWARE ENGINEERING, vol. 5, no. 12, pp. 743-749, 2015 ISSN: 2277 128X.

for wallets or the Unified Payment Interface (UPI) yet. New research from cyber security firm Kaspersky Labs reveals that 52 per cent of internet users who have lost their money to cyber criminals struggle to recover the lost money.[32]

2. Inadequate laws

The laws on digital payments are vague. E-wallets are non-bank financial companies (NBFCs) so the rules that cover banks do not apply to them, while security compliance for "fintech" companies falls under Section 43 A of the Information Technology Act. Transactions between a user and a mobile wallet service provider that are merely contractual agreements can always be repudiated. There is a heightened need to legally back digital payments in India, not only to ensure the safety of consumer money but also for the safety of these companies themselves. There is no clarity as to how and who will enforce a fair decision when something goes wrong. There are no legal mechanisms available in the case of disputes pertaining to digital payments. While maintenance of security standards for fintech companies falls under the data protection law of the IT Act, the lack of an enforcement mechanism hinders any good this can do.[33]

3. Security Risks

External threats such as hacking, sniffing and spoofing expose banks to security risks. Banks are also exposed to internal risks especially frauds by employees. Lack of knowledge amongst people to use e-banking facilities is the major constraint in India. Lack of adequate knowledge and skills is a major deterrent for employees to deal with the innovative and changing technologies in banks. Training

[32] PRIYANKA SANGANI, *50 per cent victims of cybercrime struggle to recover their money: Kaspersky Labs*, THE ECONOMIC TIMES, Dated Jan 7, 2017, <//economictimes.indiatimes.com/articleshow/ 56807388.cms?utm_source =contentofinterest&utm_medium=text&utm_campaign=cppst> (Last accessed on 17/12/2018)

[33] Alnoor Peermohamed, 'India lacks laws to protect customers of digital transactions: Experts', <https://www.business-standard.com/article/economy-policy/india-lacks-laws-to-protect-customers-of-digital-transactions-experts-116120300744_1.html> (accessed on 25/09/2018)

at all levels on the changing trends in IT is the requirement of the day for the banks.[34]

4. Liability in bank digital transactions

Bank digital transactions can go wrong due to a variety of reasons, many of them because of no fault of customers. The hacking of debit cards and bank accounts is not uncommon. With the increased use of digital payments, customers need to be protected from unauthorised banking transactions. Today, the *onus* is on customers and not the banks when banks are really in control of the payment system and are charging customers for digital transactions.[35]

5. Overcharging/stealth charges

While digital financial transformation has been rapid all over the world, led by the tech evangelists, policymakers all over the world usually think of the customers last.[36] In India, the government has taken more initiatives to build-up use of the roadmap of e-banking, which has now become a compulsory mode of banking. Banks are frequently increasing charges and reducing choices, easily justifying them in the name of digital transformation.

V. Conclusion:

Cybercriminals are using different means to steal one's bank information and ultimately their money as well.[37] A collective consensus of banks and regulators to make policies and adopt measures is inevitable to protect banking platforms from cyber threats.[38] The following are some suggestions to improve cyber security in the banking sector:

---

[34] DR. PREMCHAND NARWARE, *E-Banking – Challenges & Policy Implications*, INTERNATIONAL JOURNAL OF ENTERPRISE COMPUTING AND BUSINESS SYSTEMS, Vol. 6, Issue 2 (July – Dec. 2016)

[35] PRATIK BHAKTA, *'Frauds going up in number, banks need to tighten cyber security norms: RBI'* (2017) <//economictimes.indiatimes.com/articleshow/59388328.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst> (last accessed on 10/09/2018).

[36] DEBASHISH, *'Digital banking and its 4 BIG issues'*, <http://www.rediff.com/business/column/column-digital-banking-and-its-4-big-issues/20170410.htm> (accessed on 29/09/2018)

[37] Choo, '*The cyber threat landscape: Challenges and future research directions*. *Computers & Security'*, 308: 719-731.

[38] Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. Measuring the cost of cybercrime (2012).

1. Enactment of Legislations

The traditional law enforcement policies, standards and methods have been proved insufficient to cater to the evolving cybercrimes and the IT Act of India has been marked down time and again. There is no specific enactment that deals with cyber crimes, in particular with the Banking Sectors. The major impact of these crimes is left unsolved many a times, therefore an Act has to be enforced to curb this kind of menace. Strict statutory laws need to be passed by the Legislatures keeping in mind the interest of customers. The laws should also provide for compensation and offenders are also to be punished.[39] IT Act should be amended accordingly to define cybercrime and also specify the cases where the Act will have extra-territorial jurisdiction. The scope of the IT Act needs to be broadened to include legal framework relating to cyber laws in India.

2. Introduce Better Enforcement Mechanisms

The law enforcement should be very rigid, and updated from time to time to keep track of such crimes. There should be fast track mobile courts to solve these cases, to meet the grievances and build confidence among the public. On 13 April 2015, it was announced that the Ministry of Home Affairs would form a committee of officials from the Intelligence Bureau, Central Bureau of Investigation, National Investigation Agency, Delhi Police and ministry itself to produce a new legal framework.[40] With the increasingly notable impact of the peril of cybercrime, it has been continuously realised that local law enforcement agencies do not have the required skills and resources to investigate incidents related to cybercrimes. Engagement of specialized cyber security professionals is a step further to derive quicker and better cybercrime investigation results.

3. Create Awareness

Non-existent or inadequate awareness campaigns further simplifies the work of the cyber criminals. Alarmingly, simple phishing attacks enjoy a success rate of 45% due to lack of awareness regarding

[39] VINAYA, CHATURVEDI, "*Cyber Crime: Technological Blight in Digital Banking in India*", IOSR JOURNAL OF BUSINESS AND MANAGEMENT (IOSR-JBM,) p. 62

[40] FIANYI, I. D., *'Curbing cyber-crime and Enhancing e-commerce security with Digital Forensics'*, INTERNATIONAL JOURNAL OF COMPUTER SCIENCE ISSUES (Nov. 06, 2015).

the common safeguards to protect against the shrewd cyber criminals. The customer should be educated and made aware about various bank frauds and measures should be informed to them for safety mechanisms so that they do not fall prey as victims of cyber-crime. In case a bank introduces any new policy or there are any changes which are required to be followed by all banks as per RBI then, bank must inform the customer through mails or by informing the customer through telephone.[41] The awareness material should be timely updated keeping in mind the changes in the legislation and guidelines of RBI.[42] Training and Orientation programs must be conducted for the employees by the banks. The employees must be made aware about fraud prevention measures. Employees who go beyond their call of duty to prevent cyber frauds if rewarded will also enhance the work dedication.[43]

4. Strong Encryption-Decryption Methods

E-banking activities must be dealt using Secure Sockets Layer (SSL). It provides encryption link of data between a web server and an internet browser. The link makes sure that the data remains confidential and secure. In India, we follow asymmetric crypto system which requires two keys, public and private, for encryption and decryption of data.[44] For SSL connection a SSL Certificate is required which is granted by the appropriate authority under IT Act, 2000. To ensure security transactions RBI suggested for Public Key Infrastructure in Payment Systems such as RTGS, NEFT, Cheque Truncation System. According to RBI it would ensure a secure, safe and sound system of payment.[45] Wireless security solutions should also be incorporated. In cases of Denial of Service Attacks, banks should install and configure network security devices. Thus banks should tighten their security mechanisms and take appropriate countermeasures to ensure safety and privacy to bank's most valuable assets.[46]

---

[41] *Ibid.*

[42] *Ibid.*

[43] N JAMALUDDIN, '*E-Banking: Challenges and Opportunities in India*' (Proceedings of 23rd International Business Research Conference 18 - 20 November, 2013, Marriott Hotel, Melbourne, Australia)

[44] Section 3(2), Information Technology Act, 2000.

[45] *RBI for two stage verification for online banking transactions*, ECONOMIC TIMES, Mumbai, April 22, 2014.

[46] ZAHOOR, ZARKA, '*Challenges in Privacy and Security in Banking Sector and Related Countermeasures*', INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS (0975 – 8887) Vol.144 – No.3 (June, 2016) p.24.

5. Physical and Personnel Security

Banks must execute proper physical and ecosystem controls giving regards to threats, and based on the institution's unique geographical location, and neighbouring entities etc. Also when a new employee is employed then there should be a process of verification of the applicant. The level of verification may wary depending upon the position and job profile.[47]

6. Cooperation among nations to avert cyber crime

Cyberspace being transnational in nature requires cooperation among States to work together to avert cyber-crime. Although, a few treaties and implementation measures exist, a wholesome approach defining legal and technical measures and organizational capabilities is yet to take central importance for India in its goal to contribute to the global fight against cybercrime. IT Act, 2000 having extra-territorial application poses a problem in investigation, prosecution and extradition of foreign nationals. India should actively engage as part of the international cybercrime community cantered on Asia, Europe and America to seek help and also contribute to international cybercrime issues.[48]

7. Better Reporting System

Cyber-crime can be committed in any part of the globe having its impact in any corner. Every citizen should be able to identify and report cybercrimes from anywhere regardless of the country they reside in. The existing systems present in India for reporting cyber related offences involves registering complaints with the local police stations or cybercrime cells. Many Indian states have setup cybercrime cells, which monitor such crimes. In several instances, where the victims of cybercrime may not be able to report a cybercrime due to several reasons, such as staying in a remote location, unawareness regarding the place to report and privacy related issues. This tends to result in many cybercrime cases going unreported.

[47] RBI Guidelines on Information Security, Electronic Banking, Technology Risk management and Cyber Frauds, 2012.
[48] *Ibid.*

8. Cyber Fraud Council in Banks

Whenever a cyber-fraud is committed the victim should report to the Cyber Fraud Council that must be set up by in each and every bank to review, monitor investigate and report about cyber-crime. In case, such Council does not take perform or refuses to perform its duty then a provision to file an FIR must be made. The matter to be brought before such council can be of any value. RBI in its 2011 Report stated that when bank frauds are of less than one crore then it may not be necessary to call for the attention of the Special Committee Board.[49]

[49] RESERVE BANK OF INDIA, *Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds*, (Jan. 2011)

SARFAESI Act, 2002 – An overview

Shreya Devaki*

ABSTRACT:

The scope of this research project will entail a detailing of various provisions of the act and the entities created by this act. This act came into force in the year 2002. It is a legislation that was incorporated in order to help financial companies and institutions ensure quality of assets by providing various mechanisms. Before the execution of this act, various financial institutions were losing out and making losses due to the accumulation of bad assets or non-performing assets. Defaulters were taking advantage of the lacuna in the law and were refraining from addressing and rectifying their NPAs (non-performing assets).

Research Objectives:

1. To examine the need role of RBI in securitisation and reconstruction.
2. To determine the extent of powers of ARCs and ASCs.
3. To analyse provisions of the SARFAESI Act, 2002.
4. To study recent case laws with respect to SARFAESI Act, consequences of the act and changes brought forth because of the act.

Chapterization (Parts):

This project will be divided into seven parts:

Section 1: Scenario before Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002.

Section 2: Introduction to Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002.

* Year 4, Symbiosis Law School, Hyderabad, Shreya.devaki@slsh.edu.in

Section 3: Applicability of Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002.

Section 4: Recent Application of SARFAESI Act in various cases.

Chapter 5: Reserve Bank of India's role in Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest.

Hypothesis:

Whenever a scenario arises where a loan default takes place, banks can seize the securities that are in the nature of property or other immoveable assets (except agricultural land) without the intervention of the court. This process has made taking to task of loan defaulters very easy as the financial institutions do not have to be stuck in endless litigation before receiving their rightful dues.

Section 1:

Scenario before Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002:

This Act came into force in the year 2002. It is a legislation that was incorporated in order to help financial companies and institutions ensure quality of assets by providing various mechanisms. Before the execution of this Act, various financial institutions were losing out and making losses due to the accumulation of bad assets or non-performing assets. Defaulters were taking advantage of the lacuna in the law and were refraining from addressing and rectifying their NPAs (non-performing assets). The Act provided options and mechanisms for financial institutions to deal with these kind of assets in an effective manner so as to not sustain any losses. Before this Act, there was no manner or organisation or entity that had the power to deal with and dispose of Non Performing Assets and bad assets.

The financial institution had to carry this burden on their own shoulders. Due to this, there arose a need to establish entities that would deal with the securitisation of assets or the reconstruction of nonperforming assets. The Act established such entities which were

called ASCs and ARCs (Asset Securitisation Companies and Asset Reconstruction Companies). The Reserve Bank of India was to act as the regulator of these entities. The activities of these entities, their capital requirements, funding etc. would be prescribed by the Act. Therefore, it can be said that the Act through various provisions provides mechanisms to give an insulation to all assets. It addresses the interests and needs of secured creditors like banks. The following can be said to be the objectives of the Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002[1]: (SARFAESI ACT of 2002)

- The Act provides the legal framework for securitization activities in India
- It gives the procedures for the transfer of NPAs to asset reconstruction companies for the reconstruction of the assets.
- The Act enforces the security interest without Court's intervention
- The Act gives powers to banks and financial institutions to take over the immovable property that is hypothecated or charged to enforce the recovery of debt.

The previous legislation enacted for recovery of the default loans was Recovery of Debts due to Banks and Financial institutions Act, 1993. This Act was passed after the recommendations of the Narsimham Committee, were received to the government. This Act had created the forums such as Debt Recovery Tribunals and Debt Recovery Appellate Tribunals for expeditious adjudication of disputes with regard to ever increasing non-recovered dues. However, there were several loopholes in the Act and these loopholes were mis-used by the borrowers as well as the lawyers. This led the government introspect and another committee under Mr. Andhyarujina was appointed to examine banking sector reforms and consideration to changes in the legal system[2].

[1] tojo jose, WHAT IS SARFAESI ACT 2002? - INDIANECONOMY.NET INDIAN ECONOMY (2017), https://www.indianeconomy.net/splclassroom/what-is-sarfaesi-act-2002/ (last visited Oct 3, 2018).

[2] Highlights of SARFAESI Act, 2002, TAXGURU, https://taxguru.in/corporate-law/highlights-of-sarfaesi-act-2002.html (last visited Oct 3, 2018).

Under the SARFAESI ACT, the banks which transfer the assets are paid off by way of security receipts (SRs), debentures, bonds, etc as stipulated in the Act, which are subscribed to by only Qualified Institutional Investors and redeemed in due course of time. When the services of Asset Reconstruction Companies are taken by the banks that wish to terminate a non-performing asset or a bad asset, these Asset Reconstruction Companies are then deemed to be the lenders and have all the rights of the original lending banks. Currently, data shows that there are 14 ARCs in India, some of them promoted by some banks coming together. The first one was called ARCIL, sponsored by SBI, ICICI Bank, IDBI Bank and PNB.

The underlying idea of bringing into fruition ARCs under SARFAESI Act is to enable banks to clean up their balance sheets, pass on the burden of recovery to an agency which could give full-time attention to realize a higher amount than what the borrower is willing to offer and thus generally help faster resolution for all their NPAs[3].

Section 2:

Introduction to Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002:

The Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002, allows banks and financial institutions to auction properties in the form of flats and lands (residential and commercial) when borrowers who are customers of these institutions fail to repay their loans. It gives banks the option to reduce their non-performing assets and thus not make losses by adopting measures for recovery or reconstruction once securitization of the assets is done.

Whenever a scenario arises where a loan default takes place, banks can seize the securities that are in the nature of property or other immoveable assets (except agricultural land) without the intervention of the court. This process has made taking to task of loan defaulters very

[3] Indian banks & NPAs – IV: SARFAESI Act and its impact, MONEYLIFE NEWS & VIEWS, http://www.moneylife.in/article/indian-banks-and-npas-iv-sarfaesi-act-and-its-impact/26995.html (last visited Oct 3, 2018).

easy as the financial institutions do not have to be stuck in endless litigation before receiving their rightful dues. Mechanisms under the SARFAESI Act are however effective only for secured loans where bank can enforce the underlying security e.g. hypothecation, pledge and mortgages. In such cases, court intervention is not necessary, unless the security is invalid or fraudulent. However, if the asset in question is an unsecured asset, the bank would have to move the court to file civil case against the defaulters.[4]

The Act lays down certain methods for financial institutions to recover money from their borrowers' non-performing assets. These are three in number and are as follows:

1) Securitisation

2) Asset Reconstruction

3) Enforcement of the security created by the bank without any intervention by a court of law.

The process of securitisation can be described as a method wherein a kind of pooling and repacking of assets takes place. Meaning, the assets are remodeled into securities that are marketable and can be sold to investors in order to make good the bad debt. In a scenario where a bad asset or a non-performing asset has to be managed or "taken care of", the existing semi liquid asset (perhaps in the form of a bad loan) is converted into securities that can be made marketable. The ASC (Asset Securitisation Company) takes into possession these assets from the loan taker and conducts the following steps[5]:

i. Acquisition of financial assets from any originator (bank), and

ii. Raising of funds from qualified institutional buyers by issue of security receipts (for raising money) for acquiring the financial assets or

iii. Raising of funds in any prescribed manner, and

[4] Highlights of SARFAESI Act, 2002, *supra* note 2.
[5] jose, *supra* note 1.

iv. Acquisition of financial asset may be coupled with taking custody of the mortgaged land, building etc.

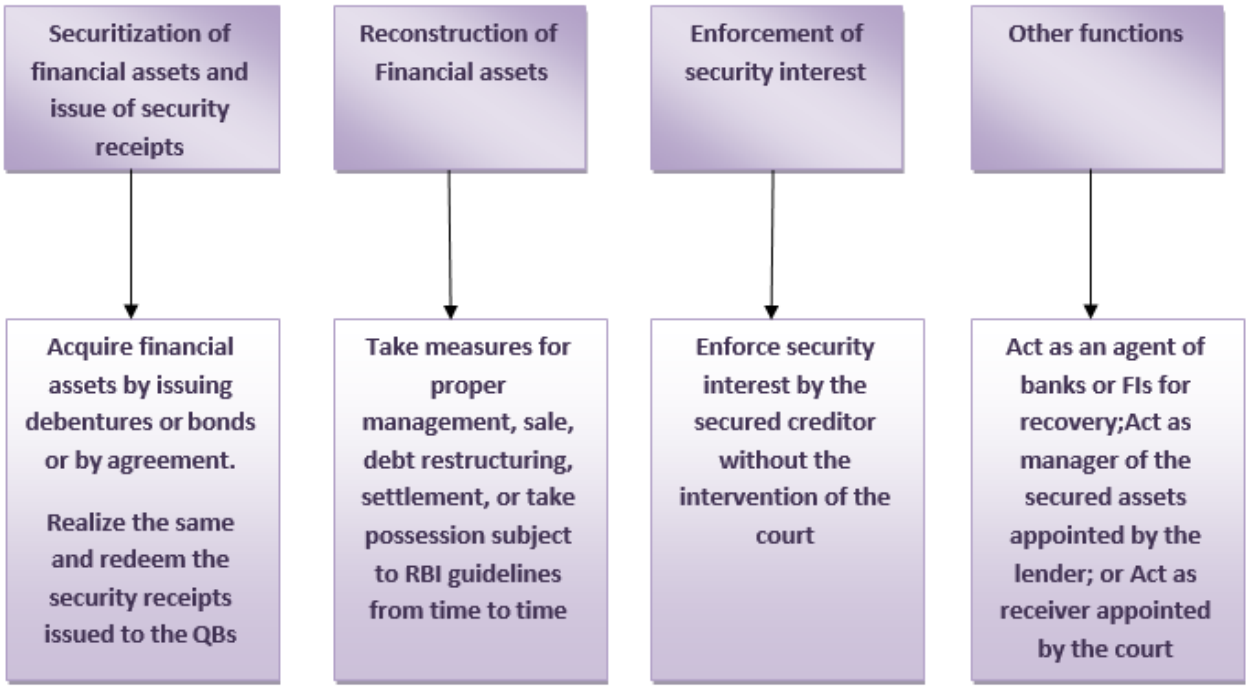
The process of asset reconstruction is one where a non performing asset is basically converted into a performing asset. This process involves an Asset Reconstruction Company that first purchases the non-performing asset. This asset is then converted into a performing asset by utilizing bonds, debentures, securities, returns from hypothecated assets and cash. Regulations laid down by the Reserve Bank of India have to be adhered to in order to validate the process of asset reconstruction. In this process, the business of the defaulter is taken over by the ARC. The business is then sold or leased out and the liabilities or debts of the defaulter are rescheduled. The interest of the securities is enforced thereby giving leave to the settlement of debts that were made by the defaulter.

The process of enforcement of securities entails the method in which a financial institution (example: a bank) issues a notice to a borrower whenever he makes a default on the loan that he has taken from the aforementioned financial institution. This notice gives the defaulting borrower 60 days time during which he is supposed to repay the debt that he owes to the institution. If the borrower continues to default the loan in spite of the notice then the financial institution according to the SARFAESI Act, 2002 has the power to enforce the interest that it has on the securities that had been put forth by the borrower when availing the loan.

Section 3:

Applicability of Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002:

Photo Credit: *Clear Tax (www.cleartax.in)*



The SARFAESI Act applies to the following[6]:

1. Facilitation of the process of securitisation of assets that have been given to financial institutions against a loan taken by a borrower.
2. Processes involving the registration and regulation by the Reserve Bank of India of asset reconstruction companies in India.
3. Process of ensuring a smooth transfer of all secured assets to securitisation and reconstruction entities so as to circumvent the involvement of courts of law.
4. Process of raising funds against non-performing assets or bad assets by issuing security receipts to qualified buyers.
5. Exercise of the power to convert non-performing assets into marketable assets.

[6] ClearTax, SARFAESI ACT, 2002- APPLICABILITY, OBJECTIVES, PROCESS, DOCUMENTATION, https://cleartax.in/s/sarfaesi-act-2002 (last visited Oct 3, 2018).

6. Classification of the borrower's account as a non-performing asset in accordance with the directions given or under guidelines issued by the Reserve Bank of India from time to time.

7. The officers authorized will exercise the rights of a secured creditor in this behalf in accordance with the rules made by the Central Government.

8. An appeal against the action of any bank or financial institution to the concerned Debts Recovery Tribunal and a second appeal to the Appellate Debts Recovery Tribunal.

9. The Act applies to all times of immoveable and moveable property (assets) except agricultural land. It also does not apply when the defaulted loan is less than rupees one lakh or when eighty percent of the loan has been repaid by the borrower.

Section 4:

Recent Application of SARFAESI Act in various cases:

- Punjab National Bank vs Raju M. Thomas[7]

  The following question was answered by the court: "*Whether guarantor can be construed as "borrower" under section 2 of the SARFAESI Act, 2002?* The guarantor is very much a 'borrower' as defined under Section2(f) of the Act which states: "borrower means any person who has been granted financial assistance by any bank or financial institution or who has given a guarantee or created any mortgage or pledge as security for the financial assistance granted by any bank or financial institution and includes a person who becomes borrower of a securitization company or reconstruction company consequent upon acquisition by it of any rights or interest of any bank or financial institution in relation to such financial assistance".[8]

[7] O.P.(DRT).No.1390 OF 2012 and O.P.(DRT).No.2835 OF 2012

[8] Manu, FRAMEWORK OF ARCS AND REAL-WORLD CASE STUDIES IN SARFAESI ACT 2002 SCHOLARTICLES (2015), https://scholarticles.wordpress.com/2015/08/28/sp1/ (last visited Oct 3, 2018).

- *Deepthi Trading Company vs. The Authorised Officer in the High Court of Madras*[9]

  Commendably, the Ruling has attempted to preserve the right to property of the borrower by ensuring that a borrower is not disposed without due process of law, the underlying premise being that secured creditors are not allowed to abuse the wide powers provided to them under the SARFAESI Act. However, this Ruling has certainly changed in favor of the borrowers. The SARFAESI Act was enacted with a distinct purpose to facilitate banks and financial institutions to recover dues in a speedy manner by enforcement of security interest without intervention of the court. The object of the debt recovery laws is to reduce non-performing assets and increase liquidity in the market.

Section 5:

Reserve Bank of India's role in Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest:

The Reserve Bank of India acts as a regulator for the asset securitisation and reconstruction companies. It supervises the acting of the companies and by virtue of this position, examines the progress and effectiveness of these companies. In order to fulfil this role, the Reserve Bank of India brought into force certain guidelines related to securitisation and reconstruction. They were issued in the year 2003. Most of the directions that were issued apply to direct acquisition of assets by an ARC or an ASC. They do not apply in cases where assets are held as a trust or for a trust. In order for these guidelines to not apply, the ASC or ARC has to settle a trust, be a trustee to such a trust and also acquire assets in the position of a trustee.

The ASCs and ARCs will become a part of the Joint Lenders' Forum as its members. Hence, they will be a part of the process that is initiated by the financial institution with respect to the stressed assets that are in question. ASCs and ARCs shall obtain prior approval of

[9] C.R.P.No.1956 of 2013

Reserve Bank when transfers of stressed assets show potential of resulting in a substantial change.

All ASCs and ARCs are required to register themselves with the RBI. Business shall commence six months from the date of receiving of permission from the RBI. The RBI shall lay down limits for every company's net owned fund. Currently, it shall not exceed 2 crores. Any SC/RC carrying on business shall have a minimum Net Owned Fund not less than fifteen percent (15%) of the total financial assets acquired or to be acquired by the SC / RC on an aggregate basis, or Rs.100 crore whichever is less. The minimum NOF shall be maintained on an ongoing basis.

In the manner described above, the RBI plays a vital role in laying down guidelines as the regulator in order to ensure smooth functioning of all ASCs and ARCs.

Bibliography:

- https://cleartax.in/s/sarfaesi-act-2002
- https://www.moneylife.in/article/how-banks-misuse-sarfaesi-act-provisions-for-loan-recovery/47625.html
- https://www.indianeconomy.net/splclassroom/what-is-sarfaesi-act-2002/
- https://taxguru.in/corporate-law/highlights-of-sarfaesi-act-2002.html
- https://corporate.cyrilamarchandblogs.com/2016/08/changing-landscape-securitisation-debt-recovery/
- https://www.moneylife.in/article/indian-banks-and-npas-iv-sarfaesi-act-and-its-impact/26995.html
- https://www.vakilno1.com/legal-news/important-judgments-on-sarfaesi-act.html
- https://scholarticles.wordpress.com/2015/08/28/sp1/#_ftn13
- https://enterslice.com/learning/function-asset-reconstruction-companies/
- https://www.rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=9901

- https://economictimes.indiatimes.com/news/economy/policy/final-guidelines-for-arc-sponsors-soon-rbi-official/articleshow/64571695.cms
- https://enterslice.com/learning/function-asset-reconstruction-companies/
- https://www.livelaw.in/tag/sarfaesi-act/

Section-V

Prevention of Frauds in Banks

FUGITIVE ECONOMIC OFFENDERS ACT, 2018 – A CRITICAL ANALYSIS

Balaji A.P.*

ABSTRACT:

The Fugitive Economic Offenders Act, 2018 is the latest Indian standard in empowering authorities to attach and confiscate properties and assets of economic offenders like loan defaulters who flee the country. It greatly enhances the power of Enforcement Directorate to deter fugitive economic offenders to evade legal process in India and flee the country, and confiscate assets of such absconders till they present themselves in stands of courts. The Act is expected to re-establish the rule of law with respect to the fugitive economic offenders as they would be forced to return to India to face trial for scheduled offences. This would likewise encourage the banks and other money related establishments to accomplish higher recuperation from financial defaults submitted by such Fugitive Economic Offenders, enhancing the financial strength of such foundations. It may be mentioned that the non-conviction-based asset confiscation for corruption-related cases is enabled under provisions of United Nations Convention against Corruption (Ratified by India in 2011). This piece examines whether the said methods in FEO Act pass the Test of Constitutionality. The authors identify the contours of the "test of reasonable classification" and "test of arbitrariness and vagueness in state action" from the perspective of Fundamental Rights jurisprudence in India with respect to the cases where the total value involved in such offences is Rs.100 crore or more, will come under the purview of this Act. In the light of bar on civil claims, so declared as FEO by the Special Court, limits the right of the impugned persons from seeking access to justice, this provision would come under the purview of Compelling State

* School of Excellence in Law.

Interest in order to withstand the Test of Constitutionality Under Art 21. The bar on the FEO/LLP/Company under the impugned provision has the effect of disabling him/it from having access to any form of civil justice both as its seeker or its respondent also has its implications in Insolvency and Bankruptcy proceedings. The author concludes that the Act will pass the test of Constitutionality. Thus, The Fugitive Economic Offenders Act, 2018 aims to tackle a peril of today that has far reaching implications upon the core of investor confidence and the well-being of the economy.

INTRODUCTION:

Over the years, India has witnessed several economic offenders flee the country anticipating criminal action or during pendency of any on-going criminal proceedings. In the recent past, the rich Indian brigade has caught the public eye on account of what the Indian Government refers to as the '*loot and scoot*' crimes. From cricket event organizers, liquor barons to diamond merchandisers all have been accused of multi crore scams and the tendency of suddenly leaving the shores of India. As per the 2015 data produced by National Crime Records Bureau, the number of economic offences in India has doubled in the last decade.[1] With the need to provide an effective, expeditious and constitutionally permissible deterrent to ensure that such actions are curbed, the Government of India introduced the Fugitive Economic Offenders Act, 2018. The Fugitive Economic Offenders Act, 2018 ("**FEOA**") was introduced by the Ministry of Finance and Corporate Affairs, which has been passed by the Lok Sabha on 19.07.2018 and subsequently by the Rajya Sabha on 25.07.2018. FEOA has received the Presidents' assent on 31.07.2018.

THE LEGISLATIVE VACUUM WHICH THE FEOA SEEKS TO FILL:

In the past, several laws have been enacted to regulate financial discipline and recovery of monies in case of delinquencies and irregularities.

[1] Economic offences double in past 10 years, NCRB data shows in the last 10 years, the reporting of economic crimes such as cheating and criminal of trust, has doubled Last Published: Fri, Oct 07 2016 in the Mint.

- SARFAESI[2] provides that if the borrower failed to discharge his liability then the banks without intervention of the courts can recover the secured assets.

- RDDBFI[3] debts, secured or unsecured may be recovered by the Debt recovery tribunal. The recovery officer is authorized to recover the debt by attaching and selling the assets, arresting the debtor etc.

- IBC[4] enjoins invocation of insolvency resolution process in appropriate circumstances comprising a restructuring of the debts through the formulation of a repayment plan.

- PMLA[5] envisions for confiscation of property derived from or involved in money laundering of proceeds of crime of a scheduled offence. Under the PMLA the Enforcement Directorate is entitled to provisionally attach the property of the defaulter pending trial subject to confirmation by the adjudicating authority. On conviction in the trial, the property stands confiscated, free from all encumbrances to the Central Government. However, the provision for confiscation is available consequent to the conclusion of trial and can rarely be used expeditiously. Further, the purpose of such confiscation is as punishment for the offence committed and not strictly as a deterrent for any absconding accused to return to India.

- Section 37A of FEMA[6] stipulates that value equivalent, in India may be seized, if any foreign exchange, foreign security or immovable property is held in contravention of Section 4 of the FEMA Act. Consequently, the competent authority may confirm or set aside such confiscation. The order of the competent authority shall continue till disposal of adjudication. If during this process the person brings back the same into India the seizure may be set aside by the competent authority;

[2] The Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002
[3] The Recovery of Debts due to Banks and Financial Institutions Act, 1993
[4] Insolvency and Bankruptcy Code, 2016
[5] Prevention of Money Laundering Act, 2002
[6] Foreign Exchange Management Act, 1999

In addition to the above enactments, the Central Bank of India from time to time issued circulars where banks and financial institutions were required to submit to it the details of willful defaulters above a specified limit[7]

In spite of the above efforts, the incidence of reporting of economic offences has been on a steep rise. One may possibly attribute the reasons for such rise to the growing proximity of rich and wealthy with the powerful Centre, best described as crony capitalism. With this background and in an attempt to curb economic offenders from evading the process of Indian law by resorting to relocation to foreign jurisdiction and thereby remaining outside the jurisdiction of Indian courts, the Fugitive Economic Offenders Act, 2018 (FEO) has been enacted.FEO is developed with the objective, as the preamble states "***A Bill to provide for measures to deter economic offenders from evading the process of Indian law by remaining outside the jurisdiction of Indian courts***". The unique trait about the FEO is that it empowers the Indian Government to confiscate the property of economic offenders absconding from India until they submit to the jurisdiction of the appropriate legal forum. This attribute in the FEO has been introduced in pursuance of India's Ratification of the United Nations Convention against Corruption[8] (UNCAC) in 2011. The UNCAC is a comprehensive anti-corruption convention that includes wide range of corruption offences and aims at garnering international co-operation in criminalizing offences of corruption. The convention recommends non-conviction-based asset confiscation for corruption related cases. Asset recovery is stated explicitly as a fundamental principle of the Convention. Member countries are bound by the UNCAC to render mutual legal assistance towards prosecution of offenders as well as in tracing, freezing, and confiscating the proceeds of corruption. It is generally observed that income earned from illicit activity is routed to other country where the source of income is not questioned. Since the offender has escaped from the respective state he/she no longer can be held liable in other state due to the principle of statehood. Hence introduction of a Statue, which helps in tracking such offenders, is the need of the hour. The ambit of proceeds of crime under FEO includes

[7] Master Circular no. RBI/2015-16/100 DBR.No.CID.BC.22/20.16.003/2015-16, dated July 1, 2015
[8] UN General Assembly, United Nations Convention Against Corruption, 31 October 2003, A/58/422

the property within and outside India acquired from any criminal activity. Hence, FEO clearly aims at capturing the offender's property not only within but also outside India as well, acquired both from legitimate as well as illegitimate means.

CONSTITUTIONAL VALIDITY OF FUGITIVE ECONOMIC OFFENDERS ACT:

Test of Reasonable Classification: The FEO Act[9] brought by the State, enables the government to provide for measures to deter economic offenders from evading the process of Indian law by remaining outside the jurisdiction of Indian courts and make a reasonable classification of people based on intelligible differentia as per Article 14 of Constitution of India for successful administration of justice. While Article 14 allows reasonable classification for the purposes of legislation it forbids any sort of **class legislation**. The test of reasonable classification was laid down by SC in ***Budhan Chaudhary v. State of Bihar***[10], which provides that: (1) the classification proposed in the legislation must be founded on intelligible differentia and that; (2) there must be close nexus between the classification and the object of the Act. The expression intelligible differentia means difference capable of being understood and should be reasonable and not arbitrary.[11] It is submitted that the Act creates classification of offences based on threshold value of Rs.100 crores, as the perambulatory clause of the FEO Act sates that this is an Act for Fugitive Economic Offender, when we ferret about the term; it is defined u/s 2(f) of FEO that: "fugitive economic offender" means any individual against whom a warrant for arrest in relation to a **Scheduled Offence** has been issued by any Court….[12] So, when we trace schedule offence definition it means "…an offence specified in the Schedule, if the total value involved in such offence or offences is **one hundred crore rupees or more**;"[13]

The civil provisions deal with the issue of non-repayment of debt. While effective in serving this purpose, they make no special provisions

[9] The Fugitive Economic Offender Act, 2018.

[10] Budhan Chaudhary v. State of Bihar, AIR 1955 SC 191, also see State of W.B. v. Anwar Ali Sarkar, 1952 SCR 284

[11] M.P. JAIN, INDIAN CONSTITUTIONAL LAW, 876 (7th ed., Lexis-Nexis Butterworth Wadhwa Publications, Nagpur, 2016).

[12] Who-(i) has left India so as to avoid criminal prosecution; or
(ii) being abroad, refuses to return to India to face criminal prosecution;

[13] Sec.2 (m), Fugitive Economic Offender Act, 2018.

to deal either with: (a) high-value offenders; (b) those who might have absconded from India when any criminal case is pending. In case of such absconders, the general provision pertaining to "proclaimed offenders" under Section 82 of the Code of Criminal Procedure, 1973 may be used. Under Section 82 of the Code, a criminal court can publish a proclamation if it has reason to believe that a person against whom a warrant has been issued is absconding. Persons accused of serious offences listed in Section 82 (4), can be declared a 'proclaimed offender' after such inquiry as the Court deems fit. Under Section 83, property of the person against whom proclamation is issued within the district may be attached. If the property is outside the district, the concerned district magistrate must endorse the attachment. However this provision has certain key drawbacks when applied to high-value economic offenders. In large defaults, criminal proceedings are likely to be in several criminal courts across the country where assets are located. This multiplicity of proceedings may lead to conflicting orders of attachment by different courts. Second, a court is unlikely to attach property outside its jurisdiction in the first place without the procedure for endorsement being followed. If followed, the same is time consuming. As a result of such delays, such offenders can continue to remain outside the jurisdiction of Indian courts for a considerable period of time.[14]

There have been several instances of economic offenders fleeing the jurisdiction of Indian courts anticipating the commencement of criminal proceedings or sometimes during the pendency of such proceedings. The absence of such offenders from Indian courts has several deleterious consequences, such as, it obstructs investigation in criminal cases, it wastes precious time of courts and it undermines the rule of law in India. Further, most of such cases of economic offences involve non-repayment of bank loans thereby worsening the financial health of the banking sector in India. The existing civil and criminal provisions in law are inadequate to deal with the severity of the problem.

[14] THE FUGITIVE ECONOMIC OFFENDERS BILL, 2017: EXPLANATORY NOTE, hosted on the home page of the Department of Economic Affairs, Ministry of Finance at http://dea.gov.in/recent-update, http://pibphoto.nic.in/documents/rlink/2017/may/p201751804.pdf.

To summarise: Where a statute providing for a more drastic procedure different from the ordinary procedure covers the whole field covered by the ordinary procedure, as in ***Anwar Ali Sarkar***[15] ***case*** **and** ***Suraj Mall Mohta's case***[16] without any guidelines as to the class of cases in which either procedure is to be resorted to, the statute will be hit by Article 14. Even there, as mentioned in ***Suraj Mall Mohta case*** a provision for appeal may cure the defect. Further, in such cases if from the preamble and surrounding circumstances, as well as the provisions of the statute themselves explained and amplified by affidavits, necessary guidelines could be inferred as in ***Saurashtra case***[17]and ***Jyoti Pershad***[18] ***case*** the statute will not be hit by Article 14. Then again where the statute itself covers only a class of cases as in ***Haldar case*** **and** ***Bajoria case*** the statute will not be bad. The fact that in such cases the executive will choose which cases are to be tried under the special procedure will not affect the validity of the statute. Therefore, the contention that the mere availability of two procedures will vitiate one of them that is the special procedure is not supported by reason or authority.[19] The position under Article 14 is different. Equal protection claims under that article are examined with the presumption that the State action is reasonable and justified. This presumption of constitutionality stems from the wide power of classification which the legislature must, of necessity, possess in making laws operating differently as regards different groups of persons in order to give effect to its policies. The power of the State to regulate criminal trials by constituting different courts with different procedures according to the needs of different parts of its territory is an essential part of its police power.[20] Though the differing procedures might involve disparity in the treatment of the persons tried under them, such disparity is not by itself sufficient, in my opinion, to outweigh the presumption and establish discrimination unless the degree of disparity goes beyond

[15] State of W.B. v. Anwar Ali Sarkar, 1952 SCR 284
[16] Suraj Mall Mohta And Co v. A. V. Visvanatha Sastri , 1954 AIR 545
[17] Kathi Raning Rawat v. State of Saurashtra, AIR 1952 SC 123
[18] Jyoti Pershad v. The Administrator For The Union territory Of Delhi ,1961 AIR 1602
[19] Maganlal Chhaganlal (P) Ltd. v. Municipal Corpn. of Greater Bombay, (1974) 2 SCC 402 at page 422
[20] Missouri v. Lewis [101 US 22]

what the reason for its existence demands as, for instance, when it amounts to a denial of a fair and impartial trial.[21]

On one point our Constitution is clear and explicit, namely that no law is valid which takes away or abridges the fundamental rights guaranteed under Part III of the Constitution.[22] The basic requirement of Article 14 is fairness in action by the State and non-arbitrariness in essence of substance is the heartbeat of fair play.[23] It is further submitted that the concept of equality is a dynamic concept with many dimensions.[24] One need not confine the denial of equality to a comparative evaluation between two persons to arrive at a conclusion of discriminatory treatment. An action *per se* arbitrary itself denies equal protection of law[25] as it has now been established that 'procedure established by law' cannot be arbitrary but should be just, fair and reasonable.[26] A basic and obvious test to apply in cases to determine if the impugned act is arbitrary or not is to see whether there is any discernible principle emerging from the impugned action and if so, does it really satisfy the test of reasonableness.[27] Like any discretion exercisable by the government or public authority, change in policy must be in conformity with the ***Wednesbury***[28] reasonableness and free from arbitrariness, irrationality, bias and malice.[29] In ***Shayara Bano v Union of India and Ors.,***[30] Justice Rohington Nariman of the Supreme Court stated that *"when something is done which is excessive and disproportionate, such legislation would be manifestly arbitrary*". The expression "arbitrarily" means: in an unreasonable manner, as fixed or done capriciously or at pleasure, without adequate determining principle, not founded in the nature of things, non-rational, not done or acting according to reason or judgment, depending on the will alone.[31]

[21] Kathi Raning Rawat v. State of Saurashtra, AIR 1952 SC 123
[22] Ram Prasad Narayan Sahi v. State of Bihar, (1953) SCR 1129.
[23] Union of India v. International Trading Co., (2003) 5 SCC 437.
[24] E.P. Royappa v. State of Tamil Nadu & Ors., (1974) 3 SCC 3.
[25] A.L. Kalra v. The Project and Equipment Corp. (P) Ltd., (1984) 3 SCC 316.
[26] Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
[27] Ibid.
[28] Associated Provincial Picture Houses Ltd. v. Wednesbury Corporation, (1948) 1 KB 223.
[29] Shimnit Utsch India (P) Ltd. v. W.B. Corporation Ltd., (2010) 6 SCC 303, ¶52.
[30] Shayara Bano v. Union of India and Ors., AIR 2018 SC 567
[31] M/S Sharma Transport Rep. By Shri D.P.Sharma v. Government Of A.P. & Ors. AIR 2002 SC 322

In the present under Section 4, 5, 12(2)(b) and 13[32] of the impugned Act, the Special Court is empowered to order that ***any properties*** or benami properties other than the proceeds of the crime, in India or abroad, are to vest with the Central Government, with all rights of the properties free from all encumbrances upon the individual being declared a Fugitive Economic Offender. The term "***any property"*** is not vague and it is not arbitrary in nature. Also the attachment of properties situated abroad is in consonance with International Practice.[33] The definition of "illegally acquired properties" in clause (*c*) of Section 3 of SAFEMA is not invalid or ineffective. The application of SAFEMA to the relatives and associates [in clauses (*c*) and (*d*) of Section 2(2)] is equally valid and effective inasmuch as the purpose and object of bringing such persons within the net of SAFEMA is to reach the properties of the detenu or convict, as the case may be, wherever they are, howsoever they are held and by whomsoever they are held. They are not conceived with a view to forfeit the independent properties of such relatives and associates as explained in this judgment. The position of 'holders' dealt with by clause (*e*) of Section 2(2) is different as explained in the body of the judgment.[34]

Retrospective Nature of Law:

The Fugitive Economic Offenders Act, 2018 is a procedural law. In order to apply such laws with retrospective effect, it is clearly to be distinguished that retroactivity and retrospectiveness are two different aspects. The Act is given retroactivity consideration and not a retrospective one. Relying upon the decisions in ***BCCI v. Kochi Cricket Private Ltd***[35] and ***The Secretary Siddhartha Academy of General and Technical Education v. Appellate Authority***[36] retroactive nature is to be considered for procedural laws.

The Test for Privacy:

It is submitted that Section 8, of the Act empowers the Director or Deputy Director for search and seizure, on the basis of information in

[32] Section 12(2)(b) , Fugitive Economic Offenders Act,2018
[33] UN General Assembly, United Nations Convention Against Corruption, 31 October 2003, A/58/422
[34] Attorney General for India v. Amratlal Prajivandas, (1994) 5 SCC 54 at page 99
[35] 2018(6) SCC 287
[36] 2012(10) S.C.R

his possession. Similar provisions are present in various other Acts enacted in India and hence existence of such a provision in one act alone cannot be construed as a violation of Article 21. Section 17 of the Prevention of Money Laundering Act contains similar provisions.

It is further contended that the rules regarding search and seizure contain all safeguards that must necessarily accompany such a provision which grants such a power to the executive[37] It is can be additionally said that such provisions exist in multiple legislations in India, including the Central Goods and Services Tax Act, 2017[38] and the Prevention of Corruption Act, wherein, Police officers are allowed to inspect any Banker's books[39] Further, It is pertinent to note that Section 8 of the FEO works in tandem with multiple other provisions of the same Act, such as Section 12, whereby a special court may declare an individual an FEO upon the seized items under Section 8 based on the application filed under Section 4.

As it was held in the Privacy Judgement[40] by a nine judge bench, the right to privacy is now a fundamental right, guaranteed under Article 21 of the Constitution of India, as part of "personal liberty". The test for privacy involves a statute fulfilling the conditions required by Article 21, held in Maneka Gandhi as being "just, fair and reasonable".[41] In addition there is a fourth test of privacy claims which deserve the highest stand of scrutiny viz. "compelling state interest". It is understood from the preamble of the Act itself, the Act seeks to bring justice to large scale economic offenders who have escaped the rule of law and whose offences vastly disrupt the economy of the country, hence it can be argued that this indubitably counts as "compelling state interest".

Blanket disentitlement:

[37] THE FUGITIVE ECONOMIC OFFENDERS (FORMS, SEARCH AND SEIZURE AND THE MANNER OF FORWARDING THE REASONS AND MATERIAL TO THE SPECIAL COURT) RULES, 2018.
[38] Section 67, The Central Goods and Services Tax Act, 2017.
[39] Section 18, Prevention of Corruption Act, 1988.
[40] Justice K S Puttaswamy (Retd.) and Anr. v. Union of India and Ors. (*2017*) 10 SCC 1
[41] Maneka Gandhi v. Union of India, (1978) 1 SCC 248

Section 14[42] of the Act states that once a person has been "declared" as a fugitive economic offender, any Court or tribunal in India, in any civil proceeding before it may disallow such individual from putting forward or defending any civil claim. With this move the government hopes to protect itself and its officers from legal suits. Further, experts note that this blanket disentitlement from pursuing or defending any civil claim should be clarified and made reasonable, lest the Act gets challenged on the grounds of violation of the basic tenets of fair play.

Right to Property and Doctrine of Eminent Domain:

By virtue of the 44th amendment to the constitution the right to property is merely a constitutional right and not a fundamental right. Article 300-A was inserted repealing Articles 19(1) (f) and 31 taking away the right to property as a fundamental right. Such acquisition or confiscation cannot be done without need of such property for public purpose and for such acquisition compensation is to be paid. "Eminent Domain" is the sovereign right of the Government to acquire any property for public purpose. It is based upon two legal maxims "*saluspopuli supreme lexesto"* and *"neccesita public major estquan"*. Banks lend loan to a person based on deposits of another. The loan availed by Fugitive Economic Offenders is also out of deposits made by the public in various banks. For the repayment of such deposits it can only be done when the principal amount and interest money are recovered from him, since interests is also to be paid to the depositors. Taking into consideration of such a large amount of loan money running to several crores, the act of recovery must be considered as an act for public purpose.

Mahajan, J., in ***Bihar v Kameshwar Prasad***[43], said that the phrase "public purpose" could not be given a "precise definition and has not a rigid meaning". The phrase could not have a static and rigid definition and it was colored according to the statute and the social circumstance whereupon it was invoked. It had to be decided on a case to case basis to determine what falls under the ambit of general interest

[42] Section 14, Fugitive Economic Offenders Act, 2018
[43] State of Bihar v. Kameshwar Singh, AIR 1952 SC 252, as read in Daulant Singh Surana, supra no.6.

of the community. In the same case, S.R.Das, J. opined that the phrase was to be accorded with the DPSPs and channeled to promote public welfare. To define the phrase, all the circumstances and facets of the statute wherein it appears need to be closed examined to determine whether a public purpose has indeed been instituted. In ***Bombay v R.S.Nanji***[44] the Court opined that though the State Government was regarded as the best judge to decide whether a purpose is a public one, Courts also have the jurisdiction to determine whether the requisition passed by the Government regarding something is for public purpose is actually so or not. The Constitution bench in the **Somawanti** judgment[45] held that the Government would be the one to determine whether a specific purpose fell within the ambit of the phrase. It also held that the satisfaction for the Government regarding the same and a subsequent declaration would be final. Such a decision by the Government could only be challenged on one ground, namely, if there was colourable exercise of power by the Government, the aggrieved party could challenge it before the Court. It was also observed in ***Laxman Rao v Maharashtra***[46] that the State Government has the ultimate power to take the decision regarding what constitutes public purpose. ***In His Holiness Kesavananda Bharati Sripadagalvaru and Ors. v. State of Kerala and Anr***[47] the court observed "*any law providing for acquisition of property must be for public purpose. The intention of legislature has to be gathered mainly from the Statement of Objects and Reasons of the Act and its Preamble.*" In ***Yogendra Kumar Jaiswal v. State of Bihar***[48]the court observed that in cases involving corruption the property confiscated need not be paid compensation as such an act cannot be completely equated with acquisition. The Fugitive Economic Offenders Act, 2018 is also one such legislation of Parliament to seize, confiscate and acquire any property which is the outcome of the proceeds of economic crime, keeping in mind the public interest.

The violation of Fundamental Right of Access to Justice under the Act cannot result in the Act being struck down de-facto, as Courts must

[44] State of Bombay v. R.S.Nanji, (1956) SCR 18, as read in Daulant Singh Surana, supra no.6
[45] Somawanti v. State of Punjab, (1963) 2 SCR 774, as read in Daulant Singh Surana, supra no.6
[46] Laxman Rao Bapurao Jadhav v. State of Maharashtra, (1997) 3 SCC 493, as read in Daulant Singh Surana , Supra no.6
[47] His Holiness Kesavananda Bharati Sripadagalvaru and Ors. v. State of Kerala and Anr. (1973) 4 SCC 225 .
[48] 2016(3)SCC 183

keep in view the compelling state interest behind such a law in the ultimate analysis of Constitutionality.

CONCLUSION:

The Government needs to work with other countries towards easing the process of extradition and strengthening the mechanisms through which fugitive economic offenders are brought back within the jurisdiction of the Indian courts. The Prime Minister in his nine-pronged agenda to deal with fugitive economic offenders at the 13th G20 Summit of leading global economies[49] also indicated the Government's steps toward the same. The Act aims at forcing economic offenders to return to India to face trial for scheduled offences. It is also expected to assist the banks and other financial institutions to achieve higher recovery from financial defaults committed by such fugitive economic offenders. It is an encouraging initiative, keeping in mind that India is gearing up to bring BASEL-III reforms where Banks are forced to increase their **Capital Adequacy Ratio.**[50]

[49] https://qrius.com/g20-summit-modis-9-point-agenda-for-action-against-fugitive-economic-offenders/

[50] https://economictimes.indiatimes.com/markets/stocks/news/paathshala-capital-adequacy-under-basel-iii/articleshow/62150112.cms

EFFICIENT WAYS TO CONTROL FRAUDS IN BANKING SECTOR

NIVEDHA.P*
&
NANDHINI.P**

ABSTRACT

Banks are seen as engines that drive the operations in the financial sector, money markets and growth of an economy. However, instances of fraud in banking sector have also taken place as a result of lacunae in its administration. The instances of fraud have increased due to complexity of bank transactions and failure in observance or procedures and norms laid down in branch operations. Banking frauds constitute a considerable percentage of white collar crimes being committed by insiders and/or outsiders.

This paper explores and envisages the various measures taken by the Government of India and the regulatory body i.e. RBI to curb the menace of banking frauds. The Indian Companies Act, 2013 places emphasis on vigil mechanism to combat frauds in banks. In 2005, RBI introduced the concept of red flagged account for banks to check loans. The paper also explores the Fugitive Economic Offenders Act, 2018 which has been introduced by the Government, which seeks to confiscate the assets of the economic offenders who flee to other countries. Though it is impossible for banks to operate in zero fraud environments, proactive steps such as risk assessment and other measures are being implemented to ensure smooth functioning.

1. INTRODUCTION:

Banks are considered as the backbone of Indian economy mainly after the liberalisation and globalisation policy which was initiated in 1991. According to Singh (2005), "The Indian banking industry is unique and has no parallels in the banking history of any country in the world. After independence, the banking sector has passed through three stages: character-based lending to ideology-based lending to

* Nivedha.P, pursuing BBA LL.B (HONS); at TN Dr. Ambedkar Law University, Chennai- 113.
** Nandhini.P, B.com (HONS), pursuing LL.B (HONS); at TN Dr. Ambedkar Law University, Chennai- 113.

competitiveness-based lending‖. The rapid growth in banking sectors coupled with other factors like diversification, privatisation, and digitalisation has enlarged its area of operation. At the same time, banks face large number of frauds and scams which affects its very own existence.

The RBI has expressed concern over the quantum jump in overall frauds in the banking sector, to INR 41,000 Cr. in 2017-18 from INR 23,000 Cr. in the previous year. The number of fraud cases reported by banks, which averaged 4,500 a year in the past 10 years, increased to 5,835 in 2017-18, according to the RBI annual report. This shakes the confidence of people and other stakeholders and it's the need of the hour to take proactive steps.

1.1 STATEMENT OF PROBLEM:

While discussing bank fraud and forgeries, the following issues to be considered:

i. what are the various kinds of frauds in banking sector?

ii. what are the problems faced by banks in its administration which has its own cost associated with it?

iii. what are the main opportunities and threats of bank to adopt and implement digitalisation and technological up gradation?

iv. whether Economic Offenders Act, 2018 is a boon for the bank or is a double edged sword in its hand?

v. what efficient measures are and can be implemented by banks to overcome the menace of banking frauds?

1.2 OBJECTIVES OF THE STUDY:

The main aim of the study is to find the efficient ways of controlling banking fraud, while specific objectives are to:

i. To study Indian banking and financial system along with current processes and regulations in place.

ii. To identify issues in the current system and reasons for these issues.

iii. To suggest recommendations that can help the system tackle these issues.

iv. To recognize the mechanism of fraud prevention and detection, and their level of effectiveness.

2. REVIEW OF LITERATURE:

Jeffords (1992) examined 910 cases submitted to the "internal auditor" during the nine year period from 1981-89 to assess the specific risk factors cited in the Treadway Commission Report. Approximately 63% of the 910 cases are classified under the internal control risks. Similarly, Calderon and Green (1994) made an analysis of 114 actual cases of corporate fraud published in the "internal auditor" from 1986 to 1990. They found that limited separation of duties, false documentation, and inadequate or non-existent control account for 60% of the fraud cases. Mehrotra (2014) observed that "one of the most challenging aspects in the Indian banking sector is to make banking transactions free from electronic crime." (Pasricha P, Mehrotra S. Electronic Crime in Indian Banking, Sai Om Journal of Commerce and Management. 2014; 1(11)).

Chiezy and Onu (2013) "evaluated the impact of fraud on the performance of 24 banks in Nigeria during 2001-2011, using Pearson correlation and multiple regression analysis. They recommended that "banks in Nigeria need to strengthen their internal control systems and the regulatory bodies should improve their supervisory role." Bhasin (2011) concluded, "Frauds generally take place in banks when safeguards and procedural controls are inadequate, or when they are not carefully followed, thus providing ample opportunities to the fraudsters. Frauds are increasing and fraudsters are becoming more sophisticated and ingenious (Bhasin ML. Contribution of Forensic Accounting to Corporate Governance: An Exploratory Study of an Asian Country. International Business Management. 2016; 10(4):479-492.)

3. FRAUD

We all know that frauds and more so, the financial frauds have been in existence for a very long time. Some may be surprised, but, it is interesting to note that Kautilya, in his famous treatise "Arthashastra" penned down around 300 BC, painted a very graphic detail of what we, in modern times, term as "fraud". Kautilya describes forty ways of embezzlement, some of which are: "what is realised earlier is entered later on; what is realised later is entered earlier; what ought to be realised is not realised; what is hard to realise is shown as realised; what is collected is shown as not collected; what has not been collected is shown as collected; what is collected in part is entered as collected in full; what is collected in full is entered as collected in part; what is collected is of one sort, while what is entered is of another sort." Everyone would agree that some of the above actions continue to be the modus operandi adopted in many instances of financial fraud that have hit the headlines in recent times.[1]

3.1 DEFINITON OF FRAUD:

RBI as a statutory body has, per se, not defined the term "fraud" in its guidelines on Frauds. 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: "A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank".

According to the Association of Certified Fraud Examiners (ACFE), fraud is "a deception or misrepresentation that an individual or entity makes knowing that misrepresentation could result in some unauthorized benefit to the individual or to the entity or some other party".[2]

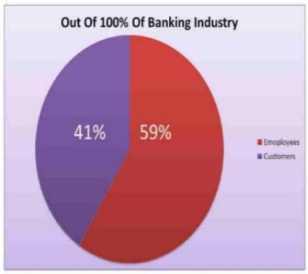
[1] https://www.bis.org/review/r130730a.pdf last accessed on 15/12/2018.
[2] https://www.ijbmi.org/papers/Vol (5)7/version-2/A05720109.pdf last accessed on 15/12/2018.

3.2 CLASSIFICATION OF FRAUD:

Banking fraud is classified by Ghosh committee as[3]

a. Fraud by insiders
b. Fraud by others.

The following statistics reveals the percentage of fraud by insiders and outsiders.



3.2.1 FRAUD BY INSIDER:

An insider threat is a malicious hacker (also called a cracker or a black hat) who is an employee or officer of a business, institution, or agency. The term can also apply to an outside person who poses as an employee or officer by obtaining false credentials. The hacker obtains access to the computer systems or networks of the enterprise and conducts activities intended to cause harm to the enterprise. In majority of cases, the insider threats can emanate from disgruntled employees or ex-employees who believe that the business, institutions or agency has "done them wrong" and feel justified in gaining revenge.

The various frauds committed by insiders are:

1. Rogue traders
2. Fraudulent loans
3. Demand draft fraud
4. Investment portfolio fraud
5. Hypothecation fraud

3.2.2 FRAUD BY OUTSIDERS:

[3] https://www.slideshare.net/mobile/Stonevinayak/frauds-in-banking last accessed on 15/12/2018.

When fraud is committed by a person other than an insider, it is classified as fraud by outsiders. The outsider generally has knowledge regarding bank's financial position and other details based on which he commits fraud.

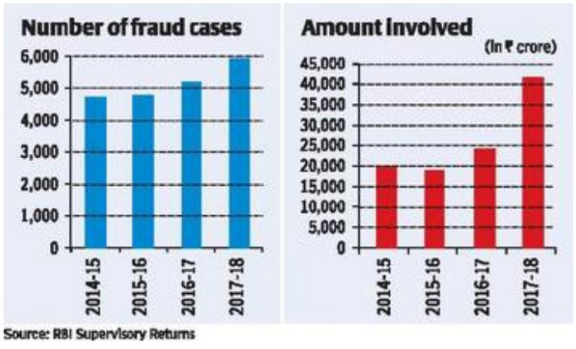
The various frauds committed by outsiders are:

1. Accounting fraud
2. Impersonation and theft of identity
3. Fraudulent loan applications
4. Phishing and Internet fraud
5. Money laundering

However, at present, large numbers of crimes are committed by outsiders along with insiders with an intention to deceive the bank.

3.3 INCIDENTS OF FRAUDS IN BANKING SECTOR:

According to recent statistical data submitted by the RBI, there has been a tremendous increase in fraud cases both in terms of number of cases and quantum of money involved.[4]



The domestic banking sector reported a total of 12,553 fraud cases worth Rs.18,170 crore in fiscal 2016-17, with state-run Bank of Maharashtra registering the highest number of such cases, says a report. While Bank of Maharashtra reported 3,893 cases of fraud, private sector lender ICICI Bank came a close second with 3,359 cases and HDFC Bank the third with 2,319 fraud cases, in the last financial year, according to proxy advisory firm Institutional Investor Advisory Services (IIAS).[5]

[4] https://www.thehindubusinessline.com/money-and-banking/not-only-npas-rbi-flags-rise-in-bank-frauds-too/article24812541.ece last accessed on 15/12/2018.

[5] https://m.economictimes.com/industry/banking/finance/banking/frauds-cost-rs-18170-crore-to-banking-sector-in-fy17-report/amp_articleshow/63535338.cms last accessed on 16/12/2018.

In terms of the quantum, Punjab National Bank (PNB) had reported the highest amount of frauds at Rs.2,810 crore in the last financial year, followed by Bank of India at Rs.2,770 crore, State Bank of India at Rs.2,420 crore and Bank of Maharashtra at Rs.2,041 crore. (et 18170 cr). Some of the instances of fraud are:[6]

1. PNB scam

On February 14 this year, the state-run lender PNB shocked the entire banking industry of India by revealing that it had been defrauded by Rs.11,400 crore allegedly by billionaire jeweler Nirav Modi, his family members and business partner Mehul Choksi, owner of the Gitanjali Gems at PNB's Brady House Branch in Mumbai. Following the scam, employees of PNB including people at the general manager level were suspended from their post for their suspected involvement in the biggest scam in the Indian banking sector. Also, the government has revoked passports of Nirav Modi and Mehul Choksi.

2. Rotomac case

Rs.3,700 Rotomac fraud was unearthed after the sensational PNB scam. The Kanpur based Rotomac Global is being probed by the CBI and Enforcement Directorate (ED) for allegedly cheating a consortium of seven banks of Rs.3,700 crore. The investigation agency filed case against Vikram Kothari and Rahul Kothari, directors of the business group for misusing credit sanctions provided by Bank of Baroda (BoB), the member of consortium banks at its International Business Branch (IBB) at The Mall Kanpur to the tune of Rs.456.63 crore.

3. SBI fraud case

State Bank of India (SBI) is at the forefront of a bank scam involving jewellery network Kanishk Gold Pvt. Ltd. (KGPL). The KGPL has been accused of defrauding a consortium of 14 banks amounting Rs.824.15 crore bank fraud led by the SBI. The Enforcement Directorate (ED) and CBI registered a case against Kanishk Gold.

4. R P Infosystem scam

[6] https://www.ibtimes.co.in/7-bank-frauds-that-have-rocked-indian-banking-sector-2018-765432 last accessed on 16/12/2018.

In January the CBI has booked two directors of R P Info Systems and its directors for allegedly cheating a consortium of banks including PNB, SBI, and Canara bank to the tune of Rs.515.15 crore. The banks alleged that loans were taken on the basis of fabricated documents.

5. PNB 91 million scam

After witnessing a scam of Rs.12,000 crore allegedly committed by Nirav Modi, the PNB has unearthed another 91 million fraud in March. It involves officials of a little-known company called Chandri Paper and Allied Products Pvt. Ltd. The fraud has been spotted at the PNB's Brady House Branch in Mumbai where the Nirav Modi scam had unfolded.

4. PREVENTIVE MEASURES TO CONTROL:

Frauds involving huge sums of money not only affects the particular bank or financial institution but will have a very big impact on the development of society. The funds will go underutilised which in turn will hamper the development of the country. The fraudsters are constantly devising new plans, updating old methods and trying out new techniques of bypassing these electronic systems meant to ensure high security of banking operations. Banks in most economies are the principal depositories of the public‘s monetary savings, the nerve centre of the payment system, the vessel endowed with the ability of money creation and allocation of financial resources and conduit through which monetary and credit policies are implemented (Idolor, 2010 and Akindele, 2011). Thus, in order to maintain the credentials of the banking sector, proper measures need to be adopted to control banking frauds though it is not possible to eliminate it completely.

Different measures have to be adopted by:

(a) the banks and financial institutions;
(b) the Government and
(c) the RBI.

4.1 MEASURES TO BE ADOPTED BY BANKS:[7]

It is the primary duty of the banks to control its internal affairs and function in a manner which is not prejudicial to the interest of its stakeholders. It should ensure proper administration and address the issues whenever they crop up. Nwanko (1991) was of the opinion that general procedures for the control should normally involve identification and detection, then lastly management.

4.1.1 FRAUD IDENTIFICATION:

Every bank should be aware of and identify the types of frauds prevalent in the society, including the international society, the causes and modalities of the frauds and the potentials and prospects of some of them occurring in the bank. This will be a function of volume, types and concentration of the banks' operations and the management control systems. There are the internal and external management controls. Internal management controls are carried out inside the company while external controls are carried out outside. Internal management control is classified into two major groups:

i. Internal Checks

Internal checks are the operational controls, which are built into the banking system to simplify the processing of entries in order to secure prompt services, to help in minimizing clerical errors and to act as insurance against collusion.

ii. Internal Audit

Internal Audit on the other hand involves the review of operations and records undertaken within a business by specifically assigned staff, which is usually the Internal Auditor. There are people called external auditors too who examine the books of the bank to determine its truth and fairness. This kind of audit is mostly statutory in nature, which is called for by the law (Onkagba 1993).

4.1.2 FRAUD PREVENTION AND DETECTION:

[7] http://ir.csuc.edu.gh:8080/xmlui/bitstream/handle/123456789/209/FRAUD.pdf?sequence=1 last accessed on 16/12/2018.

Having identified the process of fraud, the next stage is to evolve measures to prevent the occurrence of such frauds. The control systems can be classified into two, those aimed at prevention and those aimed at detection. Ekechi (1990) stated that measures aimed at fraud prevention include dual control, operational manual, establishment of inspectorate units, referencing on presentation of document of value, segregation of duties, verification of signatures, controls of dormant accounts, detection of passport sized photos, close watch on the lifestyle of staff and coding/decoding and testing of telex messages.

Measures aimed at fraud detection include checking of cashiers, call-over, reconciliation and balancing of accounts at branches, interbank at head office levels, periodical submission of statement of accounts, stock taking of security items and cash in the vaults and inspection by bank inspectors (Ojeigbede, 2000).

4.1.3 FRAUD MANAGEMENT:

In a report by the Bank of Ghana annual reports and statement of accounts, it was said that most frauds are committed by insiders usually in collusion with outside third parties, and mostly are discovered by accident or tip offs rather than internal and external auditors. The policies should stress the cardinal principles of segregation of duties to ensure that one person does not originate and complete an assignment or entry. The policy should also emphasize dual control of sensitive areas such as strong rooms and locks to security documents and account, the need for daily balancing of account and the various precautions which include necessary references for opening of accounts. Also employees should be made aware of the risks of attempting to defraud the bank and the action expected if caught. The policy should incorporate and emphasize investigation and possible prosecution of suspected frauds.

Thus to curb the instances of fraud banks should keep the 3 steps in mind i.e.,

(1) Detect
(2) Defend
(3) Evolve.

4.2 STEPS TAKEN BY THE GOVERNMENT:[8]

With the potential to become the fifth largest banking industry in the world by 2020 and third largest by 2025, India's banking and financial sector is expanding rapidly. The Indian Banking industry is currently worth Rs.81 trillion (US $ 1.31 trillion). Roughly, the **Contribution of the banking sector to GDP is about 7.7% of GDP**. Banking sector has generated employment in the economy for about 1.5 million people. It is evident from the figures that banking sector plays a crucial role in development of Indian economy and thus, it is the duty of government to protect the banks. The government has introduced many statutes, made amendments to the existing ones, has ordered proper investigation of instances of fraud, has extradited the fugitives who flew to other country, etc.

4.2.1 THE FUGITIVE ECONOMIC OFFENDERS ACT, 2018:

After the recent fraud by diamantaire Nirav Modi and Mehul Choksi to the tune of INR 13,000 Cr came into spot light and they fled the country, it became apparent that the existing provisions are not adequate to deal with the severity of the problem. This is however not the very first instance of the kind. Various fugitives flew to other countries to escape from the investigation and the trial proceedings. Thus, in order to control this recent trend, the Government initiated the bill, which was passed in the House of people on July 19, 2018 and by the council of states on July 25, 2018.

A fugitive economic offender is any individual against whom warrants for arrest are issued for the involvement in select economic offences involving amount of at least INR100 Cr or more and has left India so as to avoid criminal prosecution. The new law allows designated special court to declare a person as fugitive economic offender and to confiscate his property, including 'benami' ones. "All the rights and title in the confiscated property shall, from the date of the confiscation order, vest in the central government, free from all the encumbrances", the Act says.

[8] https://www.thehindu.com/news/national/president-nod-for-fugitive-economic-offenders-bill/article24608225.ece last accessed on 16/12/2018.

Justifying the financial limit of Rs.100 crore for invoking the provisions of this new law, Finance Minister Piyush Goyal had recently said in Parliament that it was being done to "catch the big offenders and not to clog the courts".

4.2.2 AMENDMENT IN OTHER STATUTES:

The President has also given nod to other laws - the Negotiable Instruments (Amendment) Act, 2018, the State Banks (Repeal and Amendment) Act, 2018 and the Specific Relief (Amendment) Act, 2018. The Negotiable Instruments (Amendment) Act is aimed at allowing a court to try offences related to cheque bounce expeditiously and direct the drawee to pay a minimum of 20% of the cheque amount as interim compensation.

The State Banks (Repeal and Amendment) Act is to repeal two other laws - The State Bank of India (Subsidiary Banks) Act, 1959 and the State Bank of Hyderabad Act, 1956 - and to further amend the State Bank of India Act of 1955. The Specific Relief (Amendment) Act, 2018 grants a party the right to seek damages from the other side in case of a breach of a business contract and to reduce discretion of courts in such matters. Bills in these regards were approved by Parliament recently.

4.2.3 VIGIL MECHANISM:[9]

The Indian Companies Act, 2013 introduced the concept of vigil mechanism. It is mandatory for

- All the listed companies and
- Companies which accept deposits from the public.

Companies which have borrowed money from Banks and PFI in excess of Rs.50 crores under section 177(9) read with Companies (Meetings of Board and its Powers) Rules, 2014.

[9] https://taxguru.in/company-law/whistleblowing-vigil-mechanism-companies-act-2013.html last accessed on 16/12/2018.

Companies which are required to constitute an audit committee shall operate the vigil mechanism through the audit committee and if any of the members of the committee have a conflict of interest in a given case, they should recuse themselves and the others on the committee would deal with the matter on hand. For other companies, the Board of directors shall nominate a director to play the role of audit committee for the purpose of vigil mechanism to whom other directors and employees may report their concerns.

4.3 MEASURES TAKEN BY RBI:

The Reserve Bank of India (RBI) has introduced Legal Entity Identifier or LEI. Its key aim is to check and prevent banking frauds. In fact, RBI has mandated a phase-wise implementation of LEI for all borrowers of banks in India. Entities without an LEI code will not be granted enhancement of credit facilities after a specified date.

4.3.1 LEI:

LEI is a 20 digit global reference number which uniquely identifies a company. Across the world LEI is conceived as a key measure to improve the quality and accuracy of financial data through improved risk management.

Global Legal Entity Identifier Foundation (GLEIF) is the regulator of LEI. The foundation is backed and overseen by the LEI Regulatory Oversight Committee, represented by public authorities from around the globe that have come together to jointly drive forward transparency within the global financial markets.[10]

RBI on November 2, 2017 mandate has specified introducing LEI in a phased manner for large corporate borrowers having fund and non-fund exposure of Rs.5 crore and above. Apart from LEI, the RBI has issued several guidelines which are mentioned below.

4.3.2 RBI GUIDELINES:

[10] https://www.businesstoday.in/sectors/banks/reserve-bank-of-india-legal-entity-identifier-banking-frauds-debt-loans-collateral-financial-market-central-repository-of-information-on-large-credit/story/282053.html last accessed on 16/12/2018.

According to RBI it has taken many steps to prevent fraud in banking system. Some of those steps are:

i. A framework for dealing with loan frauds of INR 50 Cr and above, under which banks classify potential fraud accounts as red flagged accounts based on observation of early warning signals, and take time bound action;

ii. An online searchable database of frauds reported by banks, in the form of Central Fraud Registry, as a tool of timely identification, control and mitigation of fraud risk and for caring out due diligence during credit sanction process;

iii. Issuance of cautions, advices by RBI, detailing names of fraudsters and their *modus operandi;*

iv. Re-verification of title deeds in respect of all credit exposers of INR 5Cr and above by banks, as mandated by RBI;

v. Issuances of various master circulars to banks, with a view to restricting imprudent practices and at the same time ensuring sound procedure for conduct of business;

vi. Requiring banks to put in place adequate audit and compliance mechanisms with board-level reporting through the Audit Committee of the Board; and

vii. Subjecting the systems and procedures in banks to supervisory review by RBI as part of the Risk Based Supervisory framework for banks.

4.3.3 SWIFT RELATED ISSUES:

As for as SWIFT (Society for World Wide Interbank Financial Telecommunication) is concerned, RBI has appraised that it had issued two circulars to banks, related to securities and operational control and SWIFT environment, in the months of August and November 2016.

- RBI has issued instructions mandating banks to implement, within stipulated deadlines, prescribed measures for strengthening the SWIFT operating environment in banks.

- Further it has constituted an Expert Committee to look into, *inter alia*, factors leading to increasing incidents of frauds in banks and measures needed to curb and prevent them and the role and effectiveness of various types of audit conducted in banks in mitigating the incidence of such frauds.

- Government has issued an advisory to Public Sector Banks to take immediate actions as per extant legal or regulatory framework to ensure that fraudulent activity is not prevailing in the bank. They have also been asked to ensure that robust systems and procedures are in place for confirming due approvals, necessary applications/documents are entered in the banks systems in respect of all letters of undertakings/comfort and SWIFT messages and ensuring scrutiny and reconciliation of nostro accounts and to take all necessary steps to safeguard against occurrence of such frauds.[11]

4.3.4 RED-FLAGGED ACCOUNTS:

With fund diversion by corporates and non-performing assets (NPAs) of banks on the rise, the RBI has decided to introduce the concept of a Red Flagged Account (RFA) in a bid to minimise fraud risks.

An RFA account is one where a suspicion of fraudulent activity is thrown up by the presence of one or more early warning signals (EWS). These signals in a loan account should immediately put the bank on alert regarding a weakness or wrong doing which may ultimately turn out to be fraudulent. “A bank cannot afford to ignore such EWS but must instead use them as a trigger to launch a detailed investigation into a RFA,” the RBI said in a circular.

[11] http://www.gstimes.in/current-affairs-rbi-has-taken-many-steps-to-prevent-frauds-in-banking-system/ last accessed on 16/12/2018.

"In particular, borrowers who have defaulted and have also committed a fraud in the account would be debarred from availing bank finance from banks and financial institutions for a period of five years from the date of full payment of the defrauded amount," it said.[12]

These are some of the measures taken by RBI to address the issue of banking frauds.

5. RECOMMENDATIONS:

The following are the recommended means of preventing bank fraud:

1. Proper vigil mechanism needs to be implemented in banks and the whistle blowers can be rewarded with an intent to encourage them to report further instances of fraud.

2. The Non-Performing Asset (NPA) is to be identified in the initial stage, so that appropriate measures can be taken at right time which in turn can protect the bank from losses.

3. Complete reliance should be placed on the policies of bank which protects the interest of its stakeholders and the employees should be made aware of the consequences if they are involved in frauds.

4. The documents are to be verified thoroughly and proper documentation must be kept on all customers.

5. Loop holes in its administration and policies are to be identified and changes are ought to be made.

6. CONCLUSION

It is indeed true that the banking sector boosts the economy and at times is considered as the indicator of development of the country. At the same time, several instances of frauds crop up each and every day which affects the integrity of banking sector. Measures are taken by the banks, government and the RBI to curb the menace of fraud. All the measures taken are to be implemented efficiently to achieve the desired

[12] https://indianexpress.com/article/business/business-others/rbi-introduces-red-flag-to-clamp-down-on-loan-frauds/ last accessed on 16/12/2018.

results. Proper awareness has to be created among public to protect them. For instance, the Association of Certified Fraud Examiners (ACFE) has championed the International Fraud Awareness Week (November 16 to 22, 2014) which is dedicated to fraud awareness, detection and prevention. Though it is not possible to eradicate and eliminate the instances of fraud, the occurrence of the event can somehow be reduced.

7. REFERENCES :

1. ASSOCHAM (2015), Current fraud trends in financial sector, joint study of Associated Chamber of Commerce and Industry of India, New Delhi and PWC.

2. Dr.K.C. Chakrabarty, Frauds in banking sector - Causes, concerns and cures - Inaugural address during the National Conference on Financial Fraud organised by ASSOCHAM, New Delhi on 26 July 2013.

3. Dmitri Koteshov, Fraud Management: Detection and prevention in banking sector, Dec. 29, 2017.

4. Ibrahim Ahmed, Mohammed D. Madawaki , Fatima Usman - Managing bank frauds and forgeries through effective control strategies, A case study of Central Bank of Nigeria, Gombe branch, Volume 3 Issue 14, April 2014, International Journal of Business and Management Invention.

5. Madan L. Bhasin, the role of technology in combatting bank frauds: Perspectives and Prospectus, Volume 5 Issue 2(9), 2016.

6. Mudit Kapoor, RBI has a new tool to prevent frauds, Business Today article, Sept. 5, 2018.

7. Nithya Nair, 7 bank frauds that have rocked Indian banking sectors in 2018, March 31, 2018 at IBT.

8. PTI, Frauds cost INR 18,170 Cr to banking sector in FY 17: RBI Report, 29 March, 2018, Economic Times.

9. PTI, President's nod for Fugative Economic Offender Bill, Aug. 05, 2018, Economic times.

10. PTI, over 23,000 bank fraud cases involving INR 1 lakh crore in 5 years, May 02, 2018.

11. Sanjay Vijaykumar, Frauds on the rise at banks, warns RBI, Aug. 29, 2018, The Hindu.

12. Sharat Sabharwal, Opacity in the banking sector, Mar. 06, 2018, The Hindu.

13. Dr. Sukhamaya Swain, Dr. Lalata Pani – frauds in Indian banking: Aspects, reasons, trends- analysis and suggestive measures, Volume 5 Issue 7, July 16.

14. https://www.bankinfosecurity.com/5-tips-to-reduce-banking-fraud-a-2534 last accessed on 15 Dec. 2018.

15. https://www.bis.org/review/r130730a.pdf last accessed on 15/12/2018.

16. https://www.businesstoday.in/sectors/banks/reserve-bank-of-india-legal-entity-identifier-banking-frauds-debt-loans-collateral-financial-market-central-repository-of-information-on-large-credit/story/282053.html last accessed on 16/12/2018.

17. https://m.economictimes.com/industry/banking/finance/banking/frauds-cost-rs-18170-crore-to-banking-sector-in-fy17-report/amp_articleshow/63535338.cms last accessed on 16/12/2018.

18. https://www.ijbmi.org/papers/Vol(5)7/version-2/ A05720109.pdf last accessed on 15/12/2018.

19. https://indianexpress.com/article/business/business-others/rbi-introduces-red-flag-to-clamp-down-on-loan-frauds/ last accessed on 16/12/2018.

20. http://ir.csuc.edu.gh:8080/xmlui/bitstream/handle/123456789/209/FRAUD.pdf?sequence=1 last accessed on 16/12/2018.

21. http://www.gstimes.in/current-affairs-rbi-has-taken-many-steps-to-prevent-frauds-in-banking-system/last accessed on 16/12/2018. 22. http://legalservicesindia.com/article/1261-bank-frauds.html last accessed on 15 Dec., 2018.

23. https://www.livemint.com/opinion/DllW1q80hhTxnOiXYU3nwM/how-banking-frauds-can-be-nipped-in-the-bud.html last accessed on 15 Dec., 2018.

24. https://www.slideshare.net/mobile/Stonevinayak/frauds-in-banking last accessed on 15/12/2018

25. https://taxguru.in/company-law/whistleblowing-vigil-mechanism-companies-act-2013.html last accessed on 16/12/2018.

26. https://www.thehindubusinessline.com/money-and-banking/not-only-npas-rbi-flags-rise-in-bank-frauds-too/article24812541.ece last accessed on 15 Dec., 2018.

ANALYSIS OF FUGITIVE ECONOMIC OFFENDER'S ACT 2018 - A STRINGENT STEP TO CURB FRAUDS

Thraptthi Perumal*

ABSTRACT:

The Parliament of India has passed the Fugitive Economic Offenders Act, 2018 in its Monsoon Session in 2018. The Act represents the Government's ambitious endeavour to buttress the multitudinous peril of economic offenders who cheat and defraud the country and its constituents only to seek haven outside of India, in an attempt to evade prosecution. The past is replete with instances of such offenders who have more or less successfully fled from justice under Indian laws subsequent to benefiting off of scams that have cost the country billions of dollars and have led to a sharp downfall in investor confidence in the country.

The Act sets out primarily by defining a "Fugitive Economic Offender" (FEO) under Section 2(f) as an individual against whom a warrant has been issued in relation to a scheduled offence under the Act and who has consequently left India to escape criminal prosecution or being abroad, refuses to return to India, to face such prosecution. The aforementioned repercussions are in the nature of, firstly, the pre-trial attachment of properties, secondly, the confiscation of potentially all of the properties of the FEO upon being declared the same and, lastly, the bar on filing or defending any civil claims before any court or tribunal in India along with similar provisions to the same effect against a company whose majority shareholder, promoter or a key managerial person is an FEO.

The relevant offences that circumstance the invocation of the Act are stipulated under the Schedule to the Act and are derived from the Indian Penal Code, 1860; the Negotiable Instruments Act, 1881; Securities and Exchange Board of India Act, 1992; Companies Act, 2013; Central Goods and Services Tax Act, 2017; etc.

* The author is currently pursuing her 7th semester, B.C.A L.L.B (Hons) at School of excellence in law, Chennai.

This paper aims to analyze the constitutional validity of the act upon repercussions on pre-trial confiscation of property that shall help the country recover its portions due to severe economic offence caused by an individual economic offender.

Legislative Competence of the Act

The intended legislation is passed considering the present economic situation of India and for the further growth of a country whose economy is fourth fastest growing thereby attracting investors from across globe, such legislations are essential to prevent offenders like Vijay Mallya escaping from the clutches of law and thereby upholding the rule of law.

Presumption in favour of constitutionality of the statute

There is always a presumption as to the constitutionality of the statute; a law will not be declared unconstitutional unless the case is so clear as to be free from doubt[1]. Additionally, it is by no means easy to impute a dishonest motive and hold that there is mala fide and malicious intention in passing the impugned Act[2]. Malice and ulterior motives cannot be attached if the Parliament has the requisite competence to enact the impugned Act and the enquiry into the motive which persuaded the Parliament into passing it would be of no relevance[3].

The presumption of constitutionality must prevail in the absence of some factual foundation of record for overthrowing the statute. Even before the concept of presumption of constitutionality could evolve into a doctrine, it was observed, "It is but a decent respect to the wisdom, integrity, and patriotism of the legislative body, by which any law is passed, to presume in favour of its validity, until its violation of the Constitution is proved beyond a reasonable doubt[4]."

[1] *V.M. Syed Mohammed & Co. v. State of Andhra,* AIR 1954 SC 314.
[2] *Kurhi Koman v. State of Kerala,* AIR 1962 SC 723.
[3] *Dharam Dutt v. Union of India,* (2004) 1 SCC 712.
[4] *A.G. v. Momodou Jobe,* (1984) 1 AC 689, 702.

It has also been observed[5] that this principle of presumption of constitutionality of a statute is but a particular application of the canon of construction embodied in the Latin Maxim, '*ut res magis val eat quam pereat*' meaning: it is better for a thing to have effect than to be made void; the construction must therefore be such as will preserve rather than destroy.

In the case of ***Kedar Nath Singh v. The State of Bihar***[6], it was held that "It is well settled that if certain provisions of law construed in one way would make them consistent with the constitution and another construction would make them unconstitutional, then Court would lean in favour of the former construction." Presumption of Constitutionality of a statute or provision is followed when two possible interpretations of a statute occur - one in violation of the Constitution and one in favour of the Constitution. In such a case, the interpretation that favours the Constitution is considered valid until the petitioner proves otherwise.

In dealing with the constitutionality of the statute, the burden of proof falls upon the petitioner to prove beyond reasonable doubt that the provision is unconstitutional. In *Charanjit Lal v. Union of India*[7], the Supreme Court has stated that the "the presumption is always in favour of the constitutionality of an enactment, and the burden is upon him who attacks it to show that there has been a clear transgression of the constitutional principles."

Hence, it is presumed that Acts made by Legislations are valid as they are the representative body of the people and accountable to them hence, are aware of their needs and act in their best interest and that they do not intend to enact a law that is *ultra vires* to the constitution. Any interpretation that creates unjust and discriminatory situation should be avoided[8].

Challenging the concept of Distribution of Powers

The Constitution of India, enumerates the Distribution of Powers between the Union and the States under Article 246 read along with VII

[5] *Hector v. Antigua and Barbados,* (1990) 2 All ER 103, 107.
[6] AIR 1962 SC 955.
[7] AIR 1951 SC 41.
[8] *Shri Ram Krishna Dalmiav Shri Justice S.R. Tendulkar and Ors*, 1958 AIR 538.

schedule of Constitution. This Act of Fugitive Economic Offenders Act, enacted by the Parliament comes within the scope of Entry 45 dealing with Banking, of the union list and hence is valid and is not unconstitutional.

In ***Calcutta Gas Ltd. v. State of West Bengal***[9] the Supreme Court has held that the 'widest possible' and 'most liberal interpretation' should be given to the language of each entry. A general word used in the entry must be construed to the extent to all ancillary or subsidiary matters which can fairly and reasonably be held to be included in it[10].

Further, Entries in the Legislative Lists are not sources of legislative power, but are merely topics or fields of legislation and must receive a liberal construction inspired by a broad[11] and generous spirit and not in a narrow and pedantic manner. Thus, entries in the lists of the Seventh Schedule, give an outline of the subject matter of legislation and should be given widest amplitude[12].

The burden is on the person who attacks constitutional validity of a law to show that there has been a transgression of the constitutional principles. The allegations regarding the violation of a constitutional principle should be specific, clear and unambiguous and it is for the person who impeaches the law as violative of a constitutional guarantee to show that the particular provision is infirm for the reasons stated by him[13].

The Centre having felt the need for strict and uniform enforcement machinery in order to put an end to offenders who have taken a loan for hundred crores and more and is evading criminal prosecution and thereby to deter such economic offenders from evading the process of law has enacted this legislation which is within its legislative competence under Entry 45 of the Union list mentioned in VII schedule of the constitution.

---

[9] *Calcutta Gas Ltd. v. State of West Bengal,* AIR 1962 SC 1044.
[10] *Prem Chand Chabra Jain v. R.K. Chabra,* (1984) 2 SCC 302.
[11] *Ujagar Prints v. Union of India,*(1989) 3 SCC 488.
[12] *Karnataka Bank Ltd. v. State of Andhra Pradesh* (2008) 2 SCC 254.
[13] *Amrit Banaspati Co. Ltd. v. Union of India,*(1995) 3 SCC 335.

3.3. The Doctrine of Colourable Legislation is not applicable

Firstly, the Doctrine of Colourable Legislation which means what cannot be done directly cannot be done indirectly, cannot be applied here as this doctrine is generally applied only as a last resort when all attempts of harmonious construction have failed. Secondly, for invoking the doctrine of Colourable Legislation, the legislature must be shown to have transgressed the limits of its constitutional power patently, manifestly and directly[14]. The onus of proof thus lies on the Petitioners to prove that the Centre has exceeded its powers directly.

In deciding the validity of a law questioned on the ground of legislative incompetence, the State can always show that the law was supportable under any other entry within the competence of the legislature. Indeed, in supporting a legislation, sustenance could be drawn and had from a number of entries. The legislation could be composite legislation drawing upon several entries[15].

Further, only when a legislature which has no power to legislate or the legislation is camouflaged in such a way as to appear within its competence when it knows it is not, then alone it can be said that the legislation so enacted is a colourable legislation and that there is no legislative competence[16]. The Centre expressly and directly has the power to make laws for the said fugitive economic offenders. This is merely an Act to deter loan defaulters from fleeing criminal prosecution and to attach their property for the loan amount.

Judicial Review and Basic Structure Doctrine

Article 13(2) of the Constitution provides that State shall not make laws inconsistent to or in violation of Fundamental rights. Any law made in contravention to Fundamental rights will be void to the extent of the contravention. The main objective of Article 13 is to secure paramountcy of Constitution especially fundamental rights[17].

[14] *State of Kerala v. People's Union for Civil liberties, Kerala State Unit,*(2009) 8 SCC 46.
[15] *Ujagar Prints v. Union of India,*(1989) 3 SCC 488.
[16] *Assistant Director of Inspection Investigation v. A.B. Shanthi,*(2002) 6 SCC 259.
[17] *Renu v. District and Sessions Judge, Tis Hazari*, AIR 1973 SC 1461.

The Acts of the legislature and the executive are scrutinized on the touchstone of the doctrine of *ultra vires*. If the act of the legislature or executive goes beyond the scope of the power entrusted to it by the Constitution, then it would be *ultra vires* and therefore void. The Constitution has entrusted law making powers to the legislature and they are required to exercise this power within the limits laid down by the Constitution under Article 13, 245 and 246.

In ***L. Chandra Kumar v. Union of India***[18], it was laid down that – "the power of judicial review over the legislative action vested in the High Court's under Article 226 and in the Supreme Court under Article 32 of the Constitution is an integral and essential feature of the constitution, constituting part of its basic structure. Hence without the power of judicial review there will be no rule of law and it would have been a mere teasing illusion and promise of unreality.

The role of the judiciary as protector of fundamental rights can be understood through the observations made in the case of ***Peerless General Finance and Investment Co. Ltd. and Anr. v. Reserve Bank of India***[19], "Wherever a statute is challenged as violative of the fundamental rights, its real effect or operation on the fundamental rights is of primary importance. It is the duty of the court to be watchful to protect the constitutional rights of a citizen as against any encroachment gradually or stealthily thereon."

The Fugitive Economic Offenders Act was enacted to uphold the rule of law i.e. to subject everyone before the courts of law equally by confiscating the property of fugitive economic offenders, which are obtained from the proceeds of crime and to deter such offenders to flee from jurisdiction of Indian Courts. Further Section 22 of the Act clearly states that this law is enacted in addition to the existing laws and not in derogation of any law in force. Also, the Act has been enacted by the legislature well within their legislative power under Article 246 of the Constitution.

[18] (1997) 3 SCC 261.
[19] (1992) 2 SCC 343.

Hence, it is humbly submitted that the impugned legislation is not violative of part III of the Constitution and is not violative of Article 13 of the Constitution and the basic structure doctrine.

Principles of natural Justice and principles of fair trial

The concept of natural justice have been defined variously. It has been taken to mean requirements of substantial justice[20], in *Vionet v. Barrett*[21], it was defined as "the natural sense of what is right and wrong" and in *Hopkins v. Smethwick Local Board of Health*[22], it was defined as "fundamental justice".

The rules of natural justice are not embodied rules and therefore it is not possible and practicable to precisely define the parameters of natural justice[23]. Its compliance depends on facts and circumstances of each case.

In *Union of India v. P.K. Roy*[24], it was held that the extent and application of the doctrine depends upon the nature of the jurisdiction conferred on the administrative authority, upon the character of the rights of the persons affected, the scheme and policy of the statute.

In *A.K. Kraipak v. Union of India*[25], the Supreme Court has observed "what particular rule of natural justice should be applied to a given case must depend on the facts and circumstances of the case, the framework of law under which the enquiry is held". Whenever a complaint is made before a court that some principles of natural justice had been contravened, the court has to decide whether the observance of that rule was necessary in the case.

It is to be noted that the principles of natural justice do not apply in case of legislative action[26]. It is also to be noted that natural justice principles can be excluded by statute but if the statute gives such a

[20] *James Dunber Smit v. Her Majesty the Queen,* (1877-78) 3 App. Cas. 614.
[21] (1885) 55 LJ RB 39.
[22] (1890) 24 QB 713.
[23] *Kumaon Mandal Vikas Nigam Ltd. v. Girja Shankar Pant,* AIR 2001 SC 24.
[24] AIR 1968 SC 850.
[25] AIR 1978 SC 597.
[26] *W.B. Electricity Regulatory Commission v. C.E.S.C. Ltd.,* AIR 2002 SC 3588.

right, it cannot be taken away. At present, the terms 'fairness and natural justice are used interchangeably[27].

This Fugitive Economic Offenders Act has been enacted primarily to uphold rule of law. Professor Dicey gives one of its facets to be equality before the law[28]. Economic offenders such as Vijay Mallya cause grave injustice to the citizens and the Government of a country by swallowing whopping amounts to the tune of several hundred crores while it is very difficult for a citizen with average income to get loans to make his ends meet. When a normal person does not repay loan, he is being treated in all inhumane way possible[29] while economic offenders like Vijay Mallya escape from the clutches of law by taking asylum[30] in other countries. To address such situation, the Government of India has enacted this legislation which is a long overdue.

The Act defines a fugitive economic offender for the first time, as a person against whom as arrest warrant has been issued for committing offences given in the Schedule of this Act and who is trying to escape from the criminal prosecution of the law by leaving India or by being abroad and refusing to come back to India[31].

Further, even when the proceeds of crime of such offenders are not able to be acquired by the government to realize the loan amount, due to lack of sufficient enactments and hence considering the need of the hour the Fugitive Economic Offenders Act, 2018 was enacted which gives power to attach the proceeds of crime i.e. any property obtained as a result of the offence done under this Act, whether in India or abroad, of the individual declared as FEC under Section 12 of the Act.

Rule of Fair Hearing: *Audi Alteram Partem.*

One of the important principles of natural justice is to hear the other side, i.e. no one should be condemned unheard. This rule insists that before passing an order against any person, reasonable opportunity of hearing must be given to him.

---

[27] Jain and Jain, Principles of Administrative Law, p. 146.
[28] Jennings- Law of the Constitution, p. 49 (3rd ed.)
[29] India today January 11, 2027- Odisha farmer beaten to death for failing to repay Loan, body chopped to pieces.
[30] Compromise para 2.
[31] Section 2 (f) of the Fugitive Economic Offenders Act, 2018.

In this case, the Impugned legislation under Section 4 clearly gives the procedure for a person to be declared as a fugitive economic offender. According to it, a director or deputy director should file an application before a special court to declare a person as a fugitive economic offender. The application must cite the reasons for believing that an individual is a fugitive economic offender.

The main ingredient of fair hearing is serving of notice. Unless a person knows the case against him, he cannot defend himself. Therefore, before the proceedings start the authority concerned is required to give the accused the notice of the case against him.

This ingredient of fair hearing is provided in Section 10 of the impugned Act wherein the special court is required to issue notice to the individual who is alleged to be a fugitive economic offender.

The Second ingredient of *Audi Alteram partem* rule is the hearing. This rule requires the other party to also be heard before passing an order. This has been adopted under Section 11 of the Fugitive Economic Offenders Act, wherein it gives the procedure for hearing an application. This section says that once the individual to whom notice is sent under Section 10 appears before the special court, then it may terminate the proceedings under this Act. The individual may also appear through his counsel with the discretion of the court.

Only when the individual fails to appear before the court despite a notice being served to him the special court proceeds to hear his case. The individual is further given a period of one week to file a reply to the application under Section 4. Only after the declaration of a person as fugitive economic offender, the proceeds of crime are confiscated, after recording the reasons in writing. Such reasoned decisions are called speaking order enabling the accused to know why the decision has been given against him. At present the requirement to give reason is considered one of the principles of natural justice[32].

In certain circumstances the rules of principles of natural justice can be excluded if it is not violative of provisions of constitution[33] and if

[32] *Siemens Engineering and Mfg. Co. v. Union of India,* AIR 1976 SC 1785.
[33] *Gullapalli Nageshwar Rao v. A.P. State Road Transport Corporation,* AIR 1959 SC 1376.

its observance would cause injury to public interest and in case of a need of prompt action or in necessity or emergency. The impugned legislation provides for pre-trial confiscation of assets as a measure to deter the offenders from escaping the clutches of law and after such confiscation the director is required to make an application under sec 4 of the Act within 30 days. Further this provision does not bar the individual from enjoyment of the property[34].

Fair Trial principle

Just as in the adversary system of trial[35] which requires the State to prove his case beyond reasonable doubt, the impugned legislation also casts the burden of proving the guilt upon the director under Section 6 of the Act. Only after the Special Court is satisfied that an individual is a FEC beyond reasonable doubt, it may declare him sounder Section 12 of the Act.

The Act further provides disentitlement of the fugitive economic offender from defending any civil claim[36]. This further ensures fair trial principle of expeditious trial. Speedy trial is an essential ingredient of reasonable, fair and just[37] procedure guaranteed under Article 21 and it is a constitutional obligation of the State to devise such a procedure as would ensure speedy trial[38]. This provision acts as a bar to the accused from instituting vexatious suits of civil claim to just delay justice.

This Act comes into play only when the alleged offender has a non-performing asset to a tune of 100 crores or more and this law covers nearly 240 kinds of economic offences. Such offenders if they flee from the jurisdiction of Indian courts, it has several toxic consequences. Firstly, it hampers investigation in criminal cases; secondly, it wastes precious time of the courts of law; third it undermines the Rule of law. This legislation treats such offenders on a more stringent note. The existing civil and criminal provisions in law are not entirely adequate to deal with the severity of the problem. It was therefore, felt necessary to provide an effective, expeditious and constitutionally permissible

[34] Sec 5 (4) of Fugitive Economic Offenders Act.
[35] *Kali Ram v. State of H.P.,* (1973) 2 SCC (cri) 1048 at p. 1059: 1974 Cri LJ 1.
[36] Sec 14 of Fugitive Economic Offenders Act, 2018.
[37] *Menaka Gandhi v Union of India,* 1978 AIR 597, 1978 SCR (2) 621.
[38] *Hussainara Khatoon v State of Bihar,* (1980) 1 SCC 98 at p. 107: 1980SCC (Cri) 40 at. P.49.

deterrent to ensure prevention of such crimes, hence this legislation defers in these aspects from the Prevention of money laundering Act, 2002, Insolvency and Bankruptcy code, 2016 which does not have provisions to deal with cross border insolvency, the Recovery of Debts due to Banks and Financial Institutions Act, 1993 and SARFAESI Act, 2002.

International perspective

The non-conviction-based asset confiscation provided under this legislation is enabled under the provisions of the **United Nations Convention against Corruption** (ratified by India in 2011) enacted to uphold Rule of law.

This law is enacted with a view to confiscate the assets of such absconders till they submit to the jurisdiction of the appropriate legal forum by empowering the concerned Indian authorities to attach and confiscate proceeds of crime and the properties of the economic offenders thereby deterring them from evading the process of law of Indian courts and forcing them to return to India to face trial for scheduled offences.

This Act was drafted after the case of Vijay Mallya came to light in order to that willful defaulters like him do not go scot-free.

Hence the impugned legislation is not only in conformity with constitutional provisions but also is in line with the principles of natural justice and fair trial principles thereby and is enacted to uphold rule of law enshrined in the Constitution.

INSURANCE INDUSTRY: AN UNEXPLORED ROUTE TO MONEY LAUNDERING

Gauri Sood*

ABSTRACT

Money laundering is not a new phenomenon, it is an age-old menace. With the passage of time, there has been a shift from the conventional methods such as entering into hawala transactions, smurfing, etc. to newer, smarter and more complicated methods of laundering of money. An example of such laundering of money is through the insurance sector. Though it is an unexplored and unhaunted route, there has been a gradual increase in money laundering in this sector. Due to the loopholes and the existence of an inadequate and ineffective preventive mechanism, the insurance industry has become vulnerable and an ideal avenue for facilitating money laundering.

This research paper aims to explore the insurance sector as a facilitating medium for money laundering, highlight loopholes in the current mechanism and provide recommendations for combating this menace.

I. Introduction:

Insurance Regulatory and Development Authority (IRDA), in its master circular on Anti-Money Laundering (AML), defines Money Laundering as "moving illegally acquired cash through the financial systems so that it appears to be legally acquired".[1]

Money laundering is an age-old menace; it has been one of the root causes for the corrosion of a nation's economic growth. When one earns and holds criminal proceeds (whether earned from terrorism, drug trafficking, smuggling, gambling, etc.) he might want to turn the same into supposedly legitimate funds/white money. This process of converting tainted money into legitimate money is called money laundering. This is done to disguise the illicit origin of the funds. The conventional ways of laundering funds include hawala transactions,

* Postgraduate Student, Gujarat National Law University, Gandhinagar.

[1] http://www.fintelekt.com/files/documents/Fintelekt-Report-AML-Insurance.pdf

smurfing, etc. Other methods of money laundering also include buying properties using names of third parties as legal owners, undervaluation of assets, overvaluation of property to obtain larger loans, establishment of shell companies, etc.

Though, with the evolution of time and rapid technological advancements, the process of detecting crimes has become easier, criminals are always two steps ahead. Therefore, new trends are emerging in money laundering over recent times. The money is laundered by criminals through different means like insurance companies, casinos, real estate, etc. However, the key focus of this paper is on money laundering through the insurance sector. Insurance industry is emerging as a popular avenue to facilitate money laundering as insurance policies are often sold by brokers or independent agents who are not directly associated with or working for the company.

The main aim of laundering money[2] is to conceal the funds and their illegal origin from the attention of legal authorities. It is carried out by executing the three-step process namely, placement, layering and integration of funds. The criminals herein try to disguise the origin of money obtained through illegal activities into the money obtained from legal sources. Otherwise they will not be able to use it, as it would connect them to the criminal activity and the law enforcement officials would seize it[3]. Money laundering has been defined as an attempt to indulge or knowingly assist or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property.[4] Money laundering can have devastating impacts on the country's economy- it facilitates criminal activities, paves way for financial crises, encourages tax evasion to name a few.

1.1 Steps involved in Money Laundering

In essence, money laundering comprises 3 stages - placement, layering and integration. The first stage is "Placement" which involves

[2] S.3, PMLA, 2002

[3] David A. Chaikin "Investigating Criminal & Corporate Money Trails". in The Money Laundering and Cash Transaction Reporting edited by Brent Fisse, David Fraser and Graeme Coss. North Ryde, NSW: Law Book Co. Pp 257-293. (1992)

[4] [S.3, Prevention of Money Laundering Act, 2002]

the disposing of criminally earned cash proceeds by depositing the amounts into a bank. It is the first stage in the process and involves movement of funds from the origin. The aim is to remove the cash from the criminal location to escape detection by legal authorities. This is executed by depositing money into a bank account opened in the name of any unknown organisation/individual. The second step is layering which involves separating the illicit criminal proceeds from their origin by the creation of a complex web of financial transactions. It erases the trail that links the funds to its owner which ensures anonymity of the same. The third stage is integration which means bringing back the laundered funds into the economy in the guise of normal business funds. At this stage, it is extremely tough to detect the illicit origin of the laundered funds.

2. Money Laundering in the Insurance Sector

2.1 Definition of Insurance

Insurance is defined as a contract whereby one person, called the insurer, undertakes to make good for the loss of another, called the insured, on payment of a specific sum of money, called premium, to him on the happening of a specified event. Thus insurance is a cooperative device to spread the loss caused by a particular risk over a number of persons who are exposed to it and who agree to insure themselves against the risk.[5]

The International Accounting Standards Boards (IASB) while circulating the International Financial Reporting Standards for Insurance (IFRS-4) in March 2004, prescribing insurance accounting and disclosure, define a contract of insurance as "a contract under which one party (that is insurer) accept significant insurance risk from another party (the policyholder) by agreeing to compensate the policyholder if a specified, uncertain future event (insured event) adversely affect the policyholder.[6]

2.2 Vulnerabilities of the Insurance Sector

[5] http://shodhganga.inflibnet.ac.in/bitstream/10603/90414/3/03_%20chapter%201.pdf
[6] http://shodhganga.inflibnet.ac.in/bitstream/10603/6538/6/06_chapter%201.pdf

The insurance sector appears to be a less haunted and explored medium for facilitating money laundering. While it seems unthinkable, insurance sector has gradually become a medium most offenders resort to launder their tainted money.

FAFT, an intergovernmental body that was established in 1989 at the G7 Summit in Paris by the Ministers of its Member Jurisdictions[7] in its report on Money Laundering and Terrorist Financing Typologies of 2004-2005 has raised and underlined various weaknesses of the Insurance Sector that could potentially subject the same to the risks of money laundering.

i) Inadequate application of AML Regulations:

A significant characteristic of the insurance sector is that most of the business is carried out by tied-agents, brokers or intermediaries, who are not directly in contact with the insurance companies. Since insurance business is carried out by both by companies as well as middlemen, AML regulations must be applied to both; however there might be inadequate application of the same. Since a larger share of the insurance market is catered to by these middlemen, it becomes difficult to subject them to the same stringent regulations as insurance companies. Also, these intermediaries must be less efficient and vigilant in exercising background checks of clients and actual source of the funds used to purchase policies. Most of these persons might not consider assuming full responsibility for exercising AML compliance as they might regard this as an obligation of only insurance companies. Usually, they are required to execute Customer Due Diligence (CDD) procedures on behalf of the insurers.

ii) Entrustment of executing CDD Procedures upon Third Parties:

Since the system of AML solely thrives on reliance upon third parties, it becomes a risky bet to ensure full and authorized verification and identification of clients and their sources of money. Intermediaries undertaking CDD procedures on behalf of the insurer they operate for may not be deemed accountable for any inadequate procedures that fail

[7] http://www.fatf-gafi.org/about/

to prevent money laundering.[8] Therefore, an inefficient and lethargic client assessment procedure characterised by poor controls, no expertise, etc. only increases the threat of money laundering in the insurance sector.

iii) Absence of AML Regulations in the field of Re-insurance and General Insurance:

Overtime, General Insurance has failed to serve as a credible source of information from the view point of Customer Due Diligence procedures. Therefore, it becomes difficult to trace the origin of funds invested by a criminal who takes up any such insurance policy using tainted funds. Also, the lack of regulations in Re-insurance sector facilitates money laundering.

iv) Market factors:

There are some specific characteristics of the insurance market that may be deemed as weaknesses. For instance, long chains of distribution facilitate breakdown, distortion and complete destruction of information received at the initial stage during compliance of CDD Procedures. This can be used to the advantage of money launderers who can easily enter the industry.

v) Gap between market advancements/developments and the AML Regulations:

While the insurance industry is classified by a rapidly growing market and is witnessing a massive change and increase in technological developments, laundering of money has become a breeze. However, the existing laws have not kept up with the advancements in technology and the existing safeguards have proved to be inadequate, a lot of criminals escape the law while successfully laundering their tainted money.

The following is an example of laundering method through the insurance sector.

[8] http://www.fintelekt.com/files/documents/Fintelekt-Report-AML-Insurance.pdf

"A person (later arrested for drug trafficking) made a financial investment (life insurance) of USD 250,000 by means of an insurance broker. He acted as follows: he contacted an insurance broker and delivered a total amount of USD 250,000 in three cash instalments. The insurance broker did not report the delivery of that amount and deposited the three instalments in the bank. These actions raise no suspicion at the bank, since the insurance broker is known to them as being connected to the insurance branch. The insurance broker delivers, afterwards, to the insurance company responsible for making the financial investment, three cheques from a bank account under his name, totalling USD 250,000, thus avoiding the raise suspicions with the insurance company.[9]*"*

3. The process of money laundering in the insurance sector

Persons who have accumulated funds from criminal means (e.g. terrorism, drug trafficking, gambling, betting, etc.) will look for avenues to invest their money. Here comes the three step process of money laundering into picture. The money launder will place the tainted funds in the economy by purchasing an insurance policy (placement). A particular area where the life insurance industry is vulnerable is the single premium product. He can do so by purchasing a policy in his name or in the name of another person, i.e. friend or relative (layering, as it erases the trail linking the funds to its actual owner). In case of the latter, the money launderer can nominate himself as the beneficiary upon the death or maturity of the insurance policy. Upon maturity of the policy or death of the policy holder, the insurance company pays the policy money to the launderer. This helps in conversion of the tainted money into white money (integration).[10]

3.1 Indicators of Money Laundering in the Insurance Sector:

There are several indicators that signify the presence or possibility of money laundering in the insurance sector, the classification of which is as follows:

i) General indicators:

[9] Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies 2002/2003, Case number 3

[10] http://shodhganga.inflibnet.ac.in/bitstream/10603/31150/9/09_chapter%203.pdf

These indicators are not just specific to the insurance industry but are also applicable to other financial transactions that suggest money laundering. These include cash transactions involving a onetime payment of a large amount. Another factor indicative of money laundering is furnishing of false or incorrect information by a party. Other indicators include rerouting of funds to foreign jurisdictions such as tax havens that relieve offenders of the burden of taxation.

ii) Nature of Policy

The conduct of a policy holder can be inferred from the nature of the policy taken. This as well as the customer's way of managing the insurance contract can serve as indicators of money laundering. Furthermore, use of funds from various different sources to pay premium is not a normal course of action and is indicative of activities at the layering or integration stage of money laundering. This holds good even when the multiple sources hint at the ownership of the policyholder. Another indicator of money laundering is payments by third parties; they act as figureheads/puppets and overshadow the real owner of funds, for the purpose of concealing the actual origin of funds. Another popular tactic used by offenders to screen funds is the practice of overpaying premium, followed by the direction/request to the insurance company to repay the surplus to a third party. Requests by customers for early redemption of the policy also indicates the possibility of money laundering, as such redemption gives legitimate colour to tainted funds. In this era of development and cut throat competition, insurance companies are striving to offer sophisticated and useful insurance products with innovative features and flexibility, such as early redemptions, partial redemptions and additional premiums. When such policies are used by customers to make additional premiums and frequent partial redemptions, it is suggestive of money laundering again.

iii) Nature and behaviour of Policyholder

A Policyholder's wholesome profile- personal, professional as well as financial provides the justification and rationale for their business relationships and transactions. While the policyholder might be genuine, nevertheless it is the duty of the insurer to verify the same.

While a man is known by the company keeps, not all policyholders having direct or indirect relationship with such criminal offenders can be accused of laundering money; however it is the responsibility of the insurer to be vigilant while executing CDD procedures. Another indication of money laundering is a policyholder's high interest in investing in single premium policies or early redemption options. Any unreasonable inclination towards such incentives can hint at the potential laundering of money. Such suspicion increases further when the customer is least concerned about any extravagant charges on early redemption. Usually offenders do not mind paying higher redemption costs as long as their tainted funds get legitimised in the process. Any other irrational or erratic behaviour of customers such as an unbelievable change in lifestyle, inconsistent and unexpected changes/modifications in the policy or unanticipated deposits or withdrawal of money, unexpected interventions of outside parties, resistance or refusal to provide information or providing incorrect/false information are also indicative of possibility of money laundering. Lastly, any undue or high difference between the customer's financial position/profile and value of insurance policy taken can raise eyebrows as to the intention of the customer.

iv) Miscellaneous indicators:

There are chances that even middlemen of insurance companies can be involved in the process of money laundering. Establishment of fake companies or shell companies or the newer counterparts of already existing insurance companies must be investigated and verified accurately to detect if they are genuine undertakings or mere shell companies that are set up to facilitate money laundering.

Sometimes, middlemen such as brokers, intermediaries or even ties agents of insurance companies may be involved in facilitating money laundering. When such middlemen join hands with offenders it becomes easier to launder money as middlemen ease out the process of client assessment and CDD. Such transactions can be detected when middlemen charge abnormally high commissions from customers.

Additionally, the IRDA has also illustrated certain transactions that are suspicious in nature, such as customer insisting on

anonymity, reluctance to provide identifying information, or providing minimal, seemingly fictitious information, Cash-based suspicious transactions for premium payment and top ups over and above Rs.5 lakhs per person per month, and multiple demand drafts each denominated for less than Rs.50,000/- frequent free look surrenders by customers, frequent request for change in address, unusual termination of policies and refunds, etc.[11]

3.2 Transactions and policy variants indicative of Money Laundering (As observed by FAFT)[12]

The various types of policies that can potentially serve as tools for money laundering include early redemption policies, single premium policies, insurance policies with a free look clause (That permit refund of premiums within the cancelation period of the contract) Transactions involving payment of premium by third parties, re routing of funds to tax havens, or payments of premium using cash only are also suggestive of laundering.

4. Laws governing insurance sector and role of regulatory bodies

4.1 An overview of the Global Perspective

The increasing concern over the invincible menace of money laundering led to the birth of the Financial Action Task Force on Money Laundering (FATF) which was established by the G-7 Summit that was held in Paris in 1989. The intergovernmental organization was entrusted with the task of studying the diverse money laundering trends and tactics, reviewing the remedial action taken up to combat the same and suggest measures that were still needed. Till date, the FAFT has given forty nine recommendations for strengthening international standards to fight money laundering as well as terrorist financing. The Financial Action Task Force (FATF) welcomed India as the FATF's 34th member country on June 25, 2010 in Amsterdam.[13]

4.2 Laws governing insurance sector and role of regulatory bodies in India

[11] http://www.fintelekt.com/files/documents/Fintelekt-Report-AML-Insurance.pdf
[12] Ibid
[13] http://www.fatf-gafi.org/

Until the year 2000, the Indian Insurance industry comprised of only two Insurers namely General Insurance Corporation of India and Life Insurance Corporation India Post 2000, there were 16 new entrants from the private sector. The Insurance Regulatory and Development Authority (IRDA) (http://www.irdaindia.org) was established by virtue of the enactment of the Insurance Regulatory & Development Authority Act in 1999. It is the regulatory authority for both life insurance as well as the general insurance businesses in India. Section 114A of the Insurance Act empowers the IRDA to frame regulations governing the insurance industry in India.

4.2.1 AML Compliance for Indian Insurance Sector

The Prevention of Money Laundering Act 2002 (PMLA) and rules there under are the source of the obligation for AML compliance for insurance companies. It is applicable to insurance companies. The IRDA via a master circular[14] in the year 2010 has specified certain steps and requirements as a part of the AML Program for all insurance companies. It requires all insurance companies to exercise certain checks, controls and execute policies to ensure AML compliance. This includes implementing the KYC policy- 'Know Your Customers' and 'Know Your Existing Customers' policies. The notification also calls for the appointment of a Principal Compliance Officer. The circular also mandated a strict system of selecting and appointing insurance agents and an even more stringent system of monitoring the same. The insurance companies are also to regulate the training of these agents and employees. FATF Recommendation No.26 requires setting up a FIU, which collects and disseminates information of suspicious activities at the national level. FIUs across the world have been set up under various departments of their nation like Police, Ministry of Finance, Central Bank or Authority of Justice.[15] The AML compliance also mandates the Audit and Inspection departments of the insurance companies to verify and ensure strict compliance with the Regulations. The IRDA has also provided for penalties such as fines and even cancellation of licence of companies that fail to meet with the requisite standards.

[14] Circular No. IRDA/F&I/CIR/AML/158/09/2010, dated 24-9-2010

[15] http://www.irdaonline.org/irdacontent/journals/irda_june06.pdf

5. Challenges in compliance of Anti-Money Laundering Regulations in India

The very fact that money laundering is still prevalent and is, in fact, growing in the field of insurance is because there are very many challenges preventing the detection of money laundering.

i) Ineffective implementation of KYC norms:

The effective implementation of KYC norms is hampered by virtue of non cooperation in furnishing of information by customers. This can be due to lack of availability of documents, or resistance or refusal by customers in providing the same on the ground of privacy. Another reason is that the third parties or agents vested with the responsibility of carrying out CDD procedures might be negligent with the same. There is also an absence of a uniform common platform or database that can record as well as store data of customers. All these factors make it difficult to detect the origin of funds and aid in screening the same.

ii) Competitive nature of insurance industry:

The struggle to survive and outnumber fellow competitors often pushes companies to sell more and more insurance products, even at the cost of facilitating laundering of funds.

iii) Participation of intermediaries in facilitating money laundering:

Easy selection and ineffective checks on the backgrounds of insurance agents make it easy for them to participate in the laundering of money. When insiders themselves are involved in the crime, it becomes easy for them to aid in screening the origin of funds.

6. Recommendations:

Due diligence and vigilance on part of insurance companies alone can help detect money laundering facilitated by customers as well as intermediaries. The author would like to provide the following suggestions on this note:

i) Implementation of KYC norms must be done more strictly:

Companies as well as agents must strive to obtain proper details about new and existing customers and issue policies only against authentic and original sources of information and documents.

ii) Prohibit sale of policies wholly or partly in exchange of cash:

Sale of policies against cash might result in selling policies for unaccounted money, the source of which might not be known and the transaction might facilitate laundering of money.

iii) Creation of database for accounting and storing customers' data:

Every company must maintain an online as well as offline record of the customer's details for a set number of years, preceding the current year. This will facilitate easy availability and access to the data of customers.

iv) Stringent selection procedure for insurance agents:

The selection process must be strengthened to verify the background of agents and they must be subject to strict monitoring to ensure that they are not at play with regard to money laundering.

v) Use of Software for Transaction Monitoring[16]:

Intelligent software applications are available specifically designed for insurance products. While selecting an application care should be taken to ensure the flexibility of such a product to ensure the adaptability of the ever developing regulatory requirements. The application should have the necessary database to support the customer profile and to add the new products. The application should be able to effectively link multiple policies to an individual and multiple individuals to a set of policies. This will help monitor transactions and initiate AML triggers at the customer or policy level. The application should also be capable of having reporting capabilities to ensure seamless compliance.[17]

7. Conclusion:

[16] http://www.fintelekt.com/files/documents/Fintelekt-Report-AML-Insurance.pdf
[17] Ibid

The business of insurance must only aim at strengthening the individual's financial position and at large the country's resources and economic growth. Therefore, in the path of economic development, the insurance industry which is a major contributor to the same must only facilitate further development and not pull the country's progress down due to the weight of money laundering.

TYPES OF BANK FRAUD AND PREVENTIVE MEASURES

DIVYA. K*

ABSTRACT:

Banks are engines that drive the operations in the financial sector, which is vital for the economy. With the nationalization of banks in 1969, they have also have emerged as engines for social change. While the operations of the bank have become increasingly significant, there is also an occupational hazard. There is a Tamil proverb, which says that *"A man who collects honey will always be tempted to lick his fingers"*. Banks are all the time dealing with money; the temptation should therefore be very high. With the rise of banking business, frauds in banking sector are also increasing and fraudsters are becoming more and more sophisticated and ingenious.

Bank fraud is the use of potentially illegal means to obtain money, assets or other property owned or held by a financial institution or to obtain money from depositors by fraudulently posing as a bank or other financial institution. It can be a fraud by banking employees (insiders) or fraud by outsiders or through a conspiracy between insiders and outsiders. Bank Fraud is a big business in today's world. It is a federal crime in many countries and sometimes considered a white collar crime. The number of bank frauds in India is substantial. 21 public sector banks have incurred losses totalling Rs.25,775 crores due to banking frauds in the financial year 2017-2018. Indian banks reported a total loss of Rs.70,000 crores due to fraud during the last three fiscals up to March 2018[1].

DEFINITION OF FRAUD:

Fraud means deceit or trickery deliberately practiced in order to gain some advantage dishonestly, it is an intentional pervasion of truth in order to induce another to part with something of value or to surrender a legal right; it is an act of deceiving or misrepresenting or cheating.

*Assistant Professor (Contract basis), School of Excellence in Law, TNDALU.

[1] www.way4indians.com/newsSearch.php

Section 17 of the Contract Act 1872 defines fraud as follows:

"Fraud means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent, with intent to deceive another party thereto or his agent, or to induce him to enter into the contract:

1) The suggestion, as a fact, of that which is not true, by one who does not believe it to be true;
2) The active concealment of a fact by one having knowledge or belief of the fact;
3) A promise made without any intention of performing it;
4) Any other act fitted to deceive;
5) Any such act or omission as the law specially declares to be fraudulent.

ESSENTIAL ELEMENTS OF FRAUD[2]

In the above statement of law, four essential elements stand out clearly as follows:

1. There must be a representation or assertion;
2. It must relate to a fact;
3. It must be with the knowledge that it is false or without belief in its truth; and
4. It must induce another to act upon the assertion in question or to do or not to do certain act.

BANK FRAUD

Bank fraud is the use of potentially illegal means to obtain money, assets, or other property owned or held by a financial institution, or to obtain money from depositors by fraudulently posing as a bank or other financial institution. In many instances, bank fraud is a criminal offence. While the specific elements of particular banking fraud may vary depending on jurisdiction, the term bank fraud applies to actions that employ a scheme or artifice, as opposed to bank robbery

[2] Principles of Banking Law and Negotiable Instruments Act-Dr.B.R.Sharma and Dr.R.P.Nainta-Pg.no.148

or theft[3]. For this reason, bank fraud is sometimes considered a white-collar crime.

CLASSIFICATION OF BANK FRAUDS:

Bank frauds have been classified as under, based mainly on the provisions of the Indian Penal Code.

a) Misappropriation and criminal breach of trust.
b) Fraudulent encashment through forged instruments, manipulation of books of account or through fictitious accounts and conversion of property;
c) Unauthorised credit facilities extended for reward or for illegal gratification.
d) Negligence and cash shortages.
e) Cheating and forgery.
f) Irregularities in foreign exchange transactions.
g) Any other type of fraud not coming under the specific heads as above;

AREAS IN WHICH FRAUDS ARE COMMITTED IN BANKS[4]

1. The forger counterfeits instruments like cheques, bank drafts, fixed deposit receipts, travellers' cheques or government securities.
2. The cheques are materially altered by raising the value of the cheques, changing the validity date or beneficiary of character of the cheques e.g. a crossed cheque is changed to a bearer cheque.
3. The signatures on cheques endorsement on collection bills, endorsements of holders of instruments, miscellaneous document like deposit receipts, vault register receipts etc are forged.

FRAUD PRONE AREAS IN DIFFERENT ACCOUNTS

In order to minimize the chances of frauds, banks have devised appropriate systems and procedures for the conduct, recording and reporting of all transactions. The following are the potential areas

[3] https://books.google.co.in/books?isbn=149706502X
[4] Dr.S.R.Myneni, Law of Banking, edition published by on 2002 (Pg.no.349)

susceptible to frauds and the preventive measures to be taken by banks to protect themselves against such frauds.

I. SAVING BANK ACCOUNTS:

The following are some of the examples of fraud being played in respect of savings bank accounts:

a) Cheques bearing the forged signatures may be presented and paid. Such frauds come to light, when the depositors call at their banks to get their passbooks updated.
b) Specimen signatures of depositors may be changed, after the death of depositors.
c) Dormant account may be operated by dishonest persons, with or without collusion of bank employees.
d) Unauthorized withdrawals from customer's accounts by employees of the bank maintaining the saving ledger and later destruction of the relevant vouchers by them.

PREVENTIVE MEASURES

The following preventive measures may be taken by the banks to counteract such frauds

a) Banks should carefully examine the signatures on cheques, withdrawal forms, letters of authority, etc. with those on record.
b) In case of illiterate depositors, the photographs should also be affixed on the account opening forms besides recording the thumb impressions. The identity of the depositor should be checked with his photograph whenever he comes for withdrawing money from his account[5].
c) Particular care should be exercised in verifying the signatures while permitting withdrawals from the accounts.
d) Presentation of passbooks should be insisted in case of non-cheque book savings bank accounts.
e) Equipment such as ultra-violet lamps and path finder's should be used in case of doubt especially when large amounts are involved.

[5] RBI/2006-07/114UBD.BPD(PCB) MC.No: 11 /13.01.000/2006-07

f) Transparent adhesive tapes on the specimen signature and other vital spots should be affixed to prevent material alteration in them.

II. CURRENT ACCOUNTS

The following types of frauds are likely to be committed in case of current accounts:

a) Opening of accounts in the name of limited companies or firms by unauthorized persons, depositing of cheques belonging to the firms or companies in such accounts, misappropriation of the money by subsequent withdrawals.
b) Presentation and payment of cheques bearing forged signatures.
c) Breach of trust by the employees of the companies or firms possessing cheque leaf duly signed by the authorised signatories[6].
d) Fraudulent alteration of the amount of the cheques and getting it paid either at the counter or through another bank.

PREVENTIVE MEASURES

In order to counteract such frauds, the bank should strictly adhere to the systems and procedures laid down for the opening of the accounts and the conduct of the transactions therein. The following points need careful attention of the banks.

a) The signature of the introducer should be properly verified and letter of thanks should be sent to him. This may help the bank particularly in those cases, where even the signature of the introducer has been forged.
b) A new account holder should be allowed to introduce another account only after the expiry of a reasonable time.
c) Blank cheque forms should be kept in proper custody and accounted for.
d) Unused cheque leaves surrendered by the customers should be effectively destroyed.
e) Specimen signature care should be kept under proper control. No tampering with them should be permitted. Particular care should be taken while recording fresh specimen signature.

[6] R. K. Dalmia vs Delhi Administration 1962 AIR 1821, 1963 SCR (1) 253

III. FRAUDS IN CASE OF INTER-BRANCH ACCOUNTS

This type of fraud can be committed only by the employees of the bank. The dishonest employee may credit his personal account by debiting the account of some branch of the bank. Such entry is detected only at the time or reconciliation of the accounts of the concerned branches. Such reconciliation is done usually after every half year. At that time, the concerned employee reverses the entry by debiting the account of some other branch and this process goes on. This type of fraud remains undetected particularly in case of branches, which have huge pending work relating to reconciliation of inter-branch transactions.

PREVENTIVE MEASURES

The following measures may considerably help in prevention of such frauds.

a) Reconciliation of inter-branch balance should be done at frequent intervals.
b) Reversal of entry should be done only with the prior permission of the branch manager.
c) The Auditors should seek confirmation of outstanding balances from the concerned branches. In case, if it is not possible to get information from all branches on account of their number being large, the confirmation may be obtained from a few branches selected on random basis[7].

IV. FRAUDS IN CASES OF REMITTANCES

In recent years, frauds in remittances viz., mail transfers, telegraphic transfers, demand drafts, etc. have become quite common. It has also been found that in many cases, the bank employees are involved in these frauds. The frauds are committed by forging the signatures of drawing official's signature, for credit of fictitious accounts already opened in advance, getting printing of demand drafts and forging the signatures of the authorized officials on them, altering the draft for a higher amount with the help of chemicals etc.

[7] RBI/2015-16/133DBS.CO.ARS.No. BC. 2/08.91.021/2015-16

Preventive Measures

a) Blank bank draft forms, blank mail transfer forms, cipher codebook, check signal apparatus should be kept in proper safe custody.
b) The paying branch/banker should carefully verify the drawing official's signatures. The Power of Attorney number, if mentioned, should also be verified.
c) Particular care should be taken when demand drafts of large amounts are being deposited in a newly opened account.
d) The paper, printing, numbering and the watermark n the demand draft should be properly checked, in case there is slightest doubt about the genuineness of the draft.

V. FRAUDS IN CASE OF ADVANCES

Following types of frauds may be committed in respect of advances:

a) Spurious gold ornaments may be pledged.
b) Sub-standard goods may be pledged with the bank or their value may be shown at inflated figures.
c) Goods or equipments charged in favour of the bank may be removed or sold away.
d) Same goods may be hypothecated in favour of different banks.

PREVENTIVE MEASURES

Following preventive measures may be taken by the bank in respect of the above frauds.

a) The credentials of the borrower as well as the bank's representatives should be thoroughly checked before they are entrusted with the job.
b) Proper inspection and regular review of the accounts should be carried out.
c) Proper control is to be exercised both over the receipt of goods as security and their delivery back to the customer. Greater care is necessary in respect of assets hypothecated with the banks, since they are not in the physical custody of the banks.

VI. FRAUDS THROUGH THE USE OF LATEST TECHNOLOGY:

The following types of bank frauds are likely to be committed by the Insiders and Outsiders through the use of latest technology[8]

Hacking: Hackers/fraudsters obtain unauthorized access to the card management system of the respective bank. Counterfeit cards are then issued for the purpose of money laundering.

Phishing: A technique used to obtain the card and personal details through a fake email

Pharming: A similar technique, where a fraudster installs malicious code on a personal computer or server. This code then redirects to another fraudulent website without the person's consent or knowledge

Vishing: Fraudsters also use the phone to solicit personal information of the customers.

Smishing: It uses cell phone text messages to lure consumers in. Often the text will contain an URL or phone number. The phone number often has an automated voice response system and again just like phishing, the smishing message usually asks for immediate attention.

Debit card skimming: A machine or camera is installed at an ATM which picks up card related information and PIN numbers when customers use their cards.

Computer viruses: With every click on the internet, a company's systems are open to the risk of being infected with nefarious software that is set up to harvest information from the company servers.

Counterfeit instruments: Fake cheques/Demand Drafts that look too good to be true are being used in a growing number of fraudulent schemes, including foreign lottery scams, cheque overpayment scams, internet auction scams and secret shopper scams.

[8] https://www.ijbmi.org/papers/Vol(5)7/version-2/A05720109.pdf

Fake apps: The first step in stealing money online is to steal information. This can be done by creating a fake app outside a play store. Hackers create fake apps which will looks exactly as the original one and the usage & interface is similar to the original app.

Mobile banking application being mapped to an incorrect mobile number: For bank customers who do not use mobile banking, an employee of the bank could attach an associate's mobile number to the bank account and install a mobile application on his mobile device. The customer's account is compromised by the associate and he or she does not get any notification about the same.

SIM Swap: The fraudsters shall first collect the personal banking information through phishing, vishing, smishing or any other means. Once they have the same, they manage to have the SIM card blocked, and obtain a duplicate one by visiting the mobile operator's retail outlet with fake identity proof. The mobile operator deactivates the genuine SIM card, which was blocked, and issues a new SIM to the fraudsters. It is now simple to generate a one-time password (OTP) required for transactions using the stolen banking information. This OTP is received on the new SIM held by the fraudsters and they can now transact before the bank customer realizes the theft and alerts the bank.

Possible frauds with Mobile Wallets[9]

Increased risk of money laundering: Transfer of money in and out of a mobile wallet (with open and semi open wallet option available) from or to a bank account is now possible. Cash-in from the bank account of an individual and cash-out to a different bank account of another individual can be used as a platform for laundering unaccounted money.

Fake merchants: If the merchant on-boarded by the service provider is a fraudster, and the payment is made by the customer for fictitious goods or services from the merchant, cash can be debited from the account. Adoption of mobile commerce is dependent on customers'

[9] The mobile wallet, which is also called mWallet, digital wallet, or eWallet, refers to a mobile technology that is used similarly to a real wallet. The Mobile Wallet provides a convenient solution for any business looking to allow customers to purchase their products online with greater ease, therefore driving sales

perceptions about how safe their virtual money is from fraud. Over time, the ability to successfully counter frauds can become a key business differentiator for mobile wallet companies. Fraud, therefore needs to be considered as a critical business risk rather than just a one-off financial loss.

PREVENTIVE MEASURES

Following preventive measures may be taken by the customers in respect of the above frauds.

a) **The account activity should be checked regularly.**

b) **The PIN and passwords should be kept secret.**

c) **A strong password should be used for online banking**.

d) **Passwords should be changed frequently.**

e) **Account info should not be given over the phone.**

f) **Account info should not be given through email.**

g) **Links embedded in emails should not be clicked.**

h) **Anti-virus protection software, firewalls and spyware blockers should be used.**

i) **Public computers should not be used for online banking.**

j) **Secure connections should be checked.**

k) **Lost cards should be reported immediately.**

l) **The surroundings at ATMs** should be made aware by the customers.

m) **Skimmers should be watched.**

n) **The receipt a**t the ATM should be taken by the customer.

RECENT BANK FRAUDS IN INDIA

Some of the biggest bank frauds that shook the country's banking system and raised several questions[10]:

2011

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

2014

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

Besides, another scam that was unfolded in 2014 was the bribe-for-loan scam involving ex-chairman and MD of Syndicate Bank SK Jain for involvement in sanctioning Rs.80 billion or Rs.8,000 crore.

In 2014, Vijay Mallya was also declared a willful defaulter by Union Bank of India and other banks such as SBI and PNB followed suit.

2015

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

2016

[10] https://www.timesnownews.com/business-economy/companies/article/bank-frauds-nirav-modi-fraud-rs-11400-crore-top-financial-institution-scams-in-india-vijay-mallya-winsome-diamonds/199024

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

2017

In 2017, Mallya's debt owing to defunct Kingfisher Airlines rose to Rs.9.5 billion or Rs.9,500 crore to IDBI and other bank branches. CBI prepared charge sheet, but he had fled the country in 2016. Currently residing in the UK, Mallya's extradition is being sought at the country's Westminster Court.

In the same year, Winsome Diamonds also known to be India's second largest corporate defaulter came under the scanner after CBI booked six cases against the group and the companies under it. This case is similar to the one observed in the fresh bank fraud involving Nirav Modi group. Letters of Undertaking were issued by Indian Banks to Jatin Mehta's Winsome Diamonds. It may be noted that, the gaps were first discovered in 2014. From mid-2013 the group failed to payback its debts, and was declared a willful defaulter by banks. The total debt amounts to almost Rs.7,000 crore.

Another case that grabbed eyeballs in the same years involved Deccan Chronicle Holdings for causing a loss of Rs.11.61 billion; CBI registered FIR against five PSBs and six charge sheets were filed against the company.

A Kolkata business tycoon Nilesh Parekh, a promoter of Shree Ganesh Jewellery House, was arrested by CBI in 2017 for causing a loss of Rs.22.23 billion to at least 20 banks. Parekh, arrested at Mumbai airport last year, allegedly defrauded banks by diverting loan money via shell companies in Hong Kong, Singapore, and the UAE.

In this case, CBI filed a case against the former zonal head of the Bank of Maharashtra and a director of a private logistics company based in Surat, owing to an alleged scam involving Rs.8.36 billion.

2018

A fresh bank fraud to the tune of Rs.11,450 crore involving diamond merchant Nirav Modi, came to light. The company, in connivance with retired employees of PNB, got at least 150 Letter of Undertakings (LoUs), allowing Nirav Modi Group to defraud the bank and many other banks who gave loans to him. An Indian Express report said that, in addition to the Rs.11,450 crore, Modi also defrauded 17 other banks of Rs.3,000 crore. In this case, however, fake LoUs were recycled by the diamond jewellery group and illegally issued to other banks for borrowing money. Nirav Modi, his family and partners have fled the country.

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

SUGGESTIONS:

Bank fraud can be counteracted by the following suggestions

a) An employee should not be allowed to remain on a particular job for an unreasonably long time. Periodical job rotation in the same branch and transfer of employees from one branch to another should be carried out.

b) Book-keeping and accounting work should not be allowed to get accumulated. Maintenance of up-to-date records help in detecting frauds quickly and discouraging fraudulent practices.

c) Personal accounts of the employees should be maintained in the same branch where they work and they should be carefully scrutinized at stipulated intervals.

d) The work of preparation of statement of accounts of customers should be done by employees other than those who are maintaining the various ledgers.

e) There should not be any unwarranted departure from normal rules and established practices.

f) The bank should carry out proper screening of the persons to be employed as well as persons to be made customers of the bank. Such screening will help the bank in detecting possible dishonest or otherwise undesirable persons.

g) A climate of honesty should be created in the organization. It should be the policy of the bank to remove the dishonest employee irrespective of his status or the type of crime committed by him. This will deter many frauds.

h) Employees should be given continuous education and training by making them familiar with current instructions and procedures, rotating of jobs, etc.

i) System and procedures laid down should be followed at all operating levels.

j) All the frauds should be reported and quickly investigated.

k) Internal audit should be carried out at regular intervals.

l) Insurance cover against various risks such as burglary, theft, fidelity of employees, cash-in-transit, etc. should be obtained.

m) As new regulations such as the Companies Act 2013 place greater emphasis on the presence of a vigil mechanism to mitigate fund risks, banks must ensure that their employees are aware of their organization's whistleblower policy and should socially ostracize those involved in frauds. They could be borrowers, lenders, staff or any other stakeholders.

CONCLUSION

Fraud is a subject that no banks want to deal with, but the reality is that most organizations experience fraud to some degree. Bank frauds are now becoming more and more constant and can be considered as one of the main reasons for disturbing the economy of the country and

with such bank frauds happening all over the country, it has become necessary to monitor these activities and if possible to create a more strict legislation to deal with these issues. It should however be noted that, bank frauds cannot be eliminated forever. Of course, they can always be prevented as well as detected. Since **'prevention is better than cure',** it will be appropriate for the banks to take preventive measures.

Section-VI

Role of RBI in regulating Banks

ROLE OF RBI IN REGULATING BANKS

K.HARI PRIYA*
&
A.LAVANYA

ABSTRACT:

Every country has a Central Bank which has control over banking system in that country. The Bank of England is the oldest Central Bank in the world. In our country, Reserve Bank of India is the Central bank and is the highest monetary institution in the country which started its operation on 1st April 1935 as share holder's bank and subsequently the Central Government on 1st January, 1949 acquired its entire capital and thus it became a state owned central bank. Reserve Bank of India [RBI] plays an important role in strengthening, developing and diversifying the country's economic and financial structure. The central bank acts as the organ of the state. The ultimate responsibility of framing and executing economic policies is that of the state, and, therefore the central bank has to advance the policies of the state. RBI represents the country in the international economic forum.

Reserve Bank of India acts as a friend, philosopher and guide to commercial banks for sound banking system in the country. The author presents how the Reserve Bank of India controls over expansion of credit, inflation through its monetary policies which are of two types quantitative or general measures, qualitative or specific measures. Quantitative measures include Bank rate policy, open market operations, variable reserve requirement etc. Qualitative measures include moral suasion, consumer credit regulation, issue of directives etc.

Introduction

A central bank is one which constitutes the apex of the monetary and banking structure of a country and which performs, in the national economic interest, various functions like regulation of currency in

* Dr. Ambedkar Global Law Institute, Tirupati

accordance with the requirement of business and general public. Central bank has the custody of cash reserve of commercial banks and also management of nation's reserves of international currency. Central bank controls credit in accordance with the needs of business with a view to carry out broad monetary policy adopted by state. In addition to it, a central bank performs some other functions to cope up with the specific requirements of the country.

The central bank acts as the organ of the state. The ultimate responsibility of framing and executing policies is that of the state and therefore the central bank has to advance the policies of the state for this purpose and act in close collaboration with finance ministry and other economic ministries of the government.

Reserve bank of India is the central and apex bank of India. Established in 1935 under the provisions of Reserve bank of India Act 1934 in Calcutta and eventually moved permanently to Mumbai. Though originally it was a private share holder's bank it was nationalised on January 1st, 1949. Reserve bank of India has been vested with extensive power to control and supervise the whole banking system in the country. It derived its powers from the Reserve Bank of India act, 1934 and The Banking Regulation Act, 1949.

Management:

The management of Reserve Bank of India is under the control of central board of directors consisting of 20 members.

a. The executive head of the bank is called Governor who is assisted by the deputy governors. They are appointed by government of India for a period of 5years. The head office of Reserve Bank of India is at Mumbai. There are four local boards at Delhi, Calcutta, Madras and Bombay.
b. These local boards are advisory in nature and government of India nominates one member each from these boards to central board.
c. There are 10 directors from various fields and one government official from the ministry of finance.

Departments of Reserve bank of India:

RBI carries outs functions smoothly and efficiently through its various departments. Some of them are:

1. **Banking department:**

   This department renders bank's services to the government and to the banks.

2. **Issue department:**

   This department's concerned with the proper and efficient management of note issue.

3. **Department of government and bank accounts:**

   This department is concerned with maintenance and supervision of the bank's accounts, annual profit and loss accounts, balance sheet etc.

4. **Exchange control department:**

   The exchange control department controls foreign exchange transactions and maintains exchange rate stability.

5. **Department of non- banking companies:**

   This department administers and controls, regulates deposits of non-banking financial companies.

Role of Reserve Bank of India:

Reserve Bank of India occupies a pivotal position in Indian economy. Reserve bank of India being the apex monetary institution, it maintains economic stability and assists growth of the economy. It gives advices to the government in its economic and financial policies and represents the country in international economic forums. It acts as a friend, philosopher and guide to commercial bank. It is the sole responsibility of Reserve bank of India for development of an adequate and sound banking system in the country, Reserve Bank of India keeps inflation under control and gives credit at cheap rates to priority sectors like the agriculture, exports and small scale industry. It protects government securities and channelizes the credit in desired directions.

As said by Dr. M.H. de Kock (Governor of Central bank of South Africa) "The guiding principle of a central bank is that it should act only in the public interest and for the welfare of the country as a whole and without regard to profit as primary consideration." So the basic principle of any central bank is to work in public interest and to make efforts to build a sound banking system.

Functions of Reserve Bank of India:

Reserve bank of India as monopoly of note-issue:

The right to issue currency notes is vested with Central bank in all the countries of the world. The right to issue notes is regulated by law. According to law, every note issued by the Reserve bank has to be backed up by an asset of equivalent volume like government securities, foreign currency and metallic reserves. This inspires public confidence in paper currency. By giving monopoly power of issuing notes to Reserve bank of India, it also ensures uniformity in the monetary system of country. The Reserve bank manages paper currency of the country in accordance with changing requirement of the economy. So there is elasticity in monetary structure of the country. The Reserve bank exercises whole control over commercial banks in creation of credit. As the creation of credit eventually depends on the volume of paper currency issued by reserve bank, it should have a check on the credit of commercial banks so that credit will not go beyond the limit such that it creates inflation in the market, and also with its monopoly power it maintains stability in internal and external values of home currency.

Reserve Bank of India as a banker, agent and adviser to the government:

As a banker to the government, the Reserve bank keeps the deposits of the central and state governments and makes payments on behalf of governments. It transacts all the general banking business of the central and state government. It accepts money on account of these governments and makes payment on their behalf and caries out other banking operations such as their exchange and remittances. To wipe away excess liquidity in the country's economy Reserve bank sells

treasury bills on behalf of central government. Reserve bank makes advances to central and state governments which are repayable within 90 days from the date of advance. It also acts as an advisory board to the government not only on banking policies and financial matters but also on a wider range of economic issues including those in the field of planning and mobilisation of resources.

Reserve Bank of India as a Banker's Bank:

Reserve bank of India got its powers to control and supervise commercial banking system as per Reserve bank of India act, 1934 and Banking regulation act, 1949; commercial banks are required by law to maintain certain minimum cash reserve ratio with the Reserve bank of India against their demand and time liabilities. It is on the basis of these reserves that the Reserve bank can transfer funds from one bank to another to facilitate the clearing of cheques. Thus Reserve bank acts as a custodian of cash reserves of commercial banks and helps to facilitate their transactions. This provision enables Reserve bank to control credit position in the country. Reserve bank is vested with power to inspect commercial banks and calls for returns and other necessary information from banks.

Reserve Bank of India as a custodian of foreign exchange reserves:

Reserve bank is required to maintain the external value of rupee. For this purpose it functions as the custodian of nation's foreign exchange reserves. It has to ensure that normal short term fluctuations in trade do not affect the exchange rate. When foreign exchange reserves are inadequate for meeting balance of payments problems it borrows from the International Monetary Fund.

RBI acts as a lender of last resort:

If the commercial banks are not able to secure financial accommodation from other sources, then, Reserve bank gives necessary credit facilities against eligible securities.

RBI as a regulator of banking system:

Reserve bank of India implements the monetary policy and monitors the functioning of banking system in India. The objective of commercial banks in country is profit oriented but the objective of reserve bank is not so. For making profits all commercial banks lend money to the borrowers through three main styles of credit or system of financing which are cash credit system, loan system, purchase and discount of bills. Since those are profitable a major portion of bank's fund is employed by way of loans and advances. The commercial banks also follow certain principles of lending to minimise the risks in business of lending. Those principles are:

a. Bankers while lending funds enquire the borrower for what purpose he is taking loan. A banker does not grant loans for speculative and unproductive purposes .They lend money only for productive purposes.
b. The bankers follow the principle of diversification of risks. They do not grant advances to few big firms only. They distribute amongst a good number of customers belonging to different trades and industries.
c. They also give loans to the borrower by seeing the position of borrower to repay the loan with interest as per the terms of contract. They always lend money to the person of integrity and having repaying capacity i.e., on security.

Reserve bank of India under Banking Regulation Act, 1949 protects the customers who approach bank for loans. When money increases in the hands of the people they start expending that money which in turn leads to increase of demand in the market. When the demand for goods in the market increases, it leads to increase of price which leads to inflation.

Excess issue of credit leads to price inflation, and ultimately to trade cycle. Possibility of earning higher rates of interest by banking institutions induces them to raise a huge structure of credit on the basis of small reserves. It encourages wastefulness on the part of individual's commercial concerns and government.

In order to control this, the Reserve bank implements monetary policy. The main concern of monetary policy is

1. To regulate monetary growth to maintain reasonable degree of price stability.
2. To ensure adequate expansion in credit to assist economic growth.
3. To encourage the flow of credit into certain desired channels including priority and the hitherto neglected sectors.

Monetary policy is implemented by the Reserve bank through the instruments of credit control. Generally two types of instruments are used to control credit.

They are (1) Quantitative or general measures.
(2) Qualitative or selective measures.

Quantitative or general measures:

The quantitative measures will have influence on total volume of credit in the banking system without special regard to, for which or for what purpose, that credit is used. They are used for changing the total volume of credit in the economy. These measures include:

a. Bank rate policy.
b. Open market operations.
c. Variable reserve requirements.
d. Repo rates and Reverse repo rates.

Bank rate policy:

This is the traditional way of controlling the credit in the economy by Reserve bank. The bank rate is the rate at which the central bank discounts the bills of commercial banks. When the Reserve bank of India wants to control credit and inflation in economy, it raises bank rate. When Reserve bank of India increases bank rate the cost of borrowing by commercial banks increases. So the commercial banks increases higher rate of interest from the borrowers. So the price of credit will increase. Increased interest rate discourages business community to borrow money as a result demand of credit will go down and investment activities, production and employment will be affected. People's purchasing power will be decreased and ultimately prices will fall. This leads to cumulative downward movement in the economy.

And when the Reserve bank of India wishes to boost production and investment activities again it decreases the bank rate which will have a reverse effect.

Open market operations:

Open market operations imply deliberate direct sales and purchases of securities, bills in the market by the Reserve Bank on its own initiative to control the volume of credit. When the central bank sells securities in the open market, other things being equal, the cash reserves of commercial banks will decrease because the commercial banks will purchase those securities from Reserve bank of India and the commercial banks will not be able to create credit which means the credit creating power of commercial banks will be reduced. So, these commercial banks again increase the rate of interest which discourage borrower to get money from banks. When Reserve bank wishes to stimulate production again it starts purchasing securities from commercial banks.

Variable reserve requirements:

The Reserve bank also uses the method of variable reserve requirements to control credit. These are two types of reserves which the commercial banks required to maintain.

1. Cash reserve ratio.
2. Statutory liquidity ratio.

Cash Reserve ratio:

It is that portion of total deposits which a commercial bank has to keep with the Reserve bank in the form of cash reserves.

Statutory liquidity ratio:

It is that portion of total deposits which a commercial bank has to keep with itself in the form of liquid assets e.g. cash, gold or approved government securities.

By changing these ratios the Reserve bank will have control over credit of commercial banks. If it wants to discourage credit in the economy it increases these ratios and it decreases these ratios if it wants to encourage credit in the economy. Rising of these rates will reduce the surplus cash reserves in banks discouraging banks to create credit. Reverse will be effects of reduction in reserve ratio requirements reflected in credit

Repo rate and Reverse repo rate:

Repo rate is the rate at which banks borrow money from central bank. Whenever banks have shortage of money they will borrow money from RBI. When Reserve bank thinks that there is surplus credit then it will increase the repo rate and discourages banks to take loans from RBI. Reserve bank increases or decreases this rate as per the situation in the markets.

Reverse repo rate is the rate at which Reserve bank borrows money from banks. An increased repo rate causes banks to transfer more funds to Reserve bank of India due to those attractive interest rates.

Qualitative or selective measures:

These measures are generally meant to regulate credit for specific purposes.

1. **Issue of directives:**

   The central bank will issue directives which are in the form of oral, written, appeals or warnings to curb individual credit structure and to restrain the aggregate volume of loans.

2. **Moral suasion:**

It is a request made by central bank to commercial banks to co-operate with the general monetary policy adopted by central bank. It is an informal form of selective credit control.

Securing loan regulation by fixation of margin requirements:

The Reserve bank is empowered to fix the margin and thereby fix the maximum amount which the purchaser of securities may borrow against those securities. If the central bank raises this margin it decreases the borrowing capacity of security holder. This is a very effective selective control device to control credit in the speculative sphere without, at the same time, limiting the availability of credit in other productive fields.

Direct action:

The central bank will take direct action against the erring commercial banks. If the banks demand credit beyond the prescribed limit it may charge a penal rate of interest over and above the bank rate.

Conclusion:

As said by Brett King, the best financial services are rendered when they happen in real time and by following the principles of mobility and ramification. In Indian banking system which is led by central bank, i.e. the Reserve bank of India, the implementation of real time principles depends on it only. Taking into consideration all the above mentioned role and leadership, it can be stated that the Indian financial system has been well served by RBI.

RBI AND ITS ROLE IN REGULATING BANKS

ASHIRWAD J.*
&
SOBIN SHAJI**

ABSTRACT

The Reserve Bank of India (RBI) is India's apex banking institution, which controls the monetary policy of the country. It started its operations on 1st April, 1935 in accordance with the Reserve Bank of India Act, 1934. The functions of a Central Bank vary from country to country with autonomous or quasi-autonomous power which regulate the vital monetary functions in the country. Its main objective is to achieve the goal of economic stability and ensuring growth of the economy. RBI is also known as the banker's bank. As a regulator and supervisor of the Indian banking system it plays many roles in respect of financial and non-financial companies. RBI derives its regulating powers for Indian Banking System from the provisions of the Banking Regulation Act 1949. The role played by RBI could be summarised through various functions such as authorising licenses to commercial banks, ensuring corporate governance in banks, maintaining reserves from the commercial banks in the form of CRR and SLR, imposing interest rates imposed by the banks, issuing prudential norms to be followed by the banks, directing banks to observe the disclosure norms, issuing guidelines with respect to KYC, AML and CFT, set up DICGC to protect small depositors by providing insurance covers, analysing the health of the banks on the basis of OSMOS etc. This paper focuses on the role played by the RBI in these areas.

* 7th Semester, BBA LLB, School of Legal Studies, CUSAT.
** 7th Semester, BCOM LLB, School of Legal studies, CUSAT.

Introduction

Reserve Bank of India, India's apex banking institution came into existence on 1st April 1935 as a private shareholders' bank. The RBI was established in accordance with the Reserve Bank of India Act 1934. Though originally privately owned, after nationalisation in 1949 the Reserve Bank became fully owned by the Government of India. The Reserve Bank's affairs are governed by a Central Board of Directors. The Board is appointed by the Government of India with respect to the Reserve Bank of India Act. The RBI performs a number of functions like formulating, implementing and monitoring the monetary policy. It acts as regulator and supervisor of the financial system of the country. In addition, the RBI also is the manager of foreign exchange. Further the RBI also plays the role as the issuer of currency, as the banker to the government and also the bank to the banker. RBI also performs a wide range of promotional functions to support national objectives. RBI lays down the broad parameters for banking operations in the country. The financial system in India includes Commercial Banks, Regional Rural Banks, Local Area Banks, Cooperative Banks, and Financial Institutions including (DFIs) and Non-Banking Financial Companies. RBI derives its regulating powers for Indian Banking System from the provisions of the Banking Regulation Act 1949. For other entities, it derives power from the RBI Act 1934. The objectives of this function are to protect the interest of the depositors and maintain the safety and soundness of the banking and financial system of the country. To keep up with the added importance of supervisory function after the liberalisation of the economy, the Board of Financial Supervision (BFS) was established in 1994. Since then BFS is acting as guiding force behind the regulatory and supervisory activities. The Relationship between RBI and Commercial Banks is that of Regulator and Regulated. By virtue of the powers conferred upon it by the Reserve Bank of India Act 1934, and the Banking regulation Act, 1949 the relationship between the Reserve Bank of India and the scheduled commercial banks is very close and of a special nature. Different ways by which the RBI regulates the commercial banks could be classified as :

- Licensing Requirements

- Corporate Governance in Banks
- Statutory Pre-emptions
- Interest Rates
- Prudential Norms
- Disclosure Norms
- Anti-Money Laundering Norms
- Protection of Small Depositors
- Para – banking Activities
- Annual Onsite Inspection
- OSMOS

Banking Regulation Act

The Banking Regulation Act, 1949 is a legislation that regulates all banking firms in India.[1] The Act provides a framework using which commercial banking in India is supervised and regulated. The Act gives the Reserve Bank of India (RBI) the power to license banks, have regulation over shareholding and voting rights of shareholders; supervise the appointment of the boards and management; regulate the operations of banks; lay down instructions for audits; control moratorium, mergers and liquidation; issue directives in the interests of public good and on banking policy, and impose penalties.[2]

Reserve Bank POF India Act 1934

Reserve Bank of India Act, 1934 is the legislative act under which the Reserve Bank of India was formed. This act was amended in the year 1936 along with the Companies Act to pave way for the effective supervision of banking firms in India. This Act also gives the RBI the right to purchase and discount bills of exchange from commercial banks. It can purchase foreign exchange from banks and sell it to them. It can also provide loans to banks and state financial corporations. Further it is possible for the RBI to provide advances to the central

[1] Dr. Ashok Sharma. Auditing. FK Publications. p. 214. ISBN 978-81-87139-74-4. Retrieved 11 January 2015.
[2] Bimal N. Patel (2008). India and International Law: Introduction. MartinusNijhoff Publishers. pp. 218–219. ISBN 90-04-16152-X. Retrieved 11 January 2015.

government and state governments. It can buy or sell government securities. It can deal in derivative, repo and reverse repo.[3]

Reserve Bank of India and Commercial Banks

RBI provides several functions to banks and in the context of the ever-increasing risks in the financial system; it is inventing new methods to ensure the safety and health of the banking system. What makes the RBI-commercial bank relationship a key factor in the economy is that the RBI is the regulator and supervisor of the commercial banking system. RBI's monetary policy has an objective called financial stability which ensures that banks should be healthy and capable of withstanding crisis. Financial stability is the most vital priority of the RBI's monetary policy especially after the global financial crisis.

Banker of Banks

In the traditional version, RBI is known as banker's bank. RBI is bank of all banks in India. As a banker of banks, RBI:

- Enables smooth and swift clearing and settlements of inter-bank transactions
- Provides efficient means of funds transfer for all banks, enables banks to maintain their accounts with RBI for statutory reserve requirements and maintenance of funds transfer for all banks
- Acts as lender of last resort (LORL)

Reserve Bank maintains current account of all other banks and provides them facility to maintain cash reserves and also to carry out inter-bank transactions. A magnificent service by the RBI to commercial banks is that the central bank settles payments between different banks. This makes the payment transactions between different banks quite easy. The RBI has two facilities called NEFT (National Electronic Fund Transfer) and RTGS (Real Time Gross Settlement) for interbank payment and settlement system.[4] RBI provides the Real Time Gross

[3] VijayaragavanIyengar (1 January 2009). Introduction to Banking. Excel Books India. pp. 155–. ISBN 978-81-7446-569-6. Retrieved 13 January 2015

[4] https://www.indianeconomy.net/splclassroom/how-the-rbi-manages-the-banking-system/

Settlement System (RTGS) facility to the banks for inter-bank transactions.[5]

Lender of the Last Resort

The banks can borrow from the RBI by keeping eligible securities as collateral or any other arrangement and at the time of need or crisis, they approach RBI for financial help. Thus RBI works as Lender of the Last Resort (LORL) for banks.

Licensing Requirements

A license from the RBI is required for a company be it from India or any foreign nation for doing the business of commercial banking in India. Opening of Branches is handled by the Branch Authorization Policy. At present, Indian banks no longer require a license from the Reserve Bank for opening a branch at a place with population of below 50,000.

Corporate Governance in Banks

One of the major objectives of RBI is to ensure high-quality corporate governance in banks. RBI has issued guidelines for 'fit and proper' criteria for the director of banks. One of these guidelines is that the directors of the banks should have special knowledge/ experience in the various banking related areas. RBI can also appoint additional directors to the board of a banking company.[6]

CRR

Under CRR a certain percentage of the total bank deposits has to be kept in the current account with RBI which means banks do not have access to that much amount for any economic activity or commercial activity. Banks can't lend the money to corporates or individual borrowers, banks can't use that money for investment purposes. So, CRR remains in current account and banks don't earn anything on that.[7] In India, every scheduled commercial bank has to

[5] https://www.gktoday.in/gk/rbi-as-banker-of-banks/
[6] https://www.gktoday.in/gk/how-rbi-regulates-commercial-banks/
[7] https://www.moneycontrol.com/news/business/personal-finance/what-is-crr-slrrepo-rate-1260507.html

keep cash reserves with the RBI. In return, the RBI provides some invaluable services to the banks including: providing payment and settlement system for banks, extending Lender of Last Resort facility to banks besides insuring the deposits (below rupees one lakh) with Deposit Insurance Corporation. The DIC is a fully owned subsidiary of the RBI.

SLR

Statutory Liquidity Ratio (SLR) is defined as 'the share of bank's total deposit that it needs to maintain itself as liquid assets'.[8] In other words the ratio of liquid assets to net demand and time liabilities (NDTL) is called statutory liquidity ratio (SLR). Apart from Cash Reserve Ratio (CRR), banks have to maintain a stipulated proportion of their net demand and time liabilities in the form of liquid assets like cash, gold and unencumbered securities. Treasury bills, dated securities issued under market borrowing programme and market stabilisation schemes (MSS), etc. also form part of the SLR. Banks have to report to the RBI every alternate Friday their SLR maintenance, and pay penalties for failing to maintain SLR as mandated.[9]

By varying Cash Reserve Ratio and Statutory Reserve Ratio RBI regulates liquidity in the market. If reserve requirements are changed banks may have more or less liquidity affecting credit creation favourably or adversely.

Interest Rates

The interest rates on most of the categories of deposits and lending transactions have been deregulated and are largely determined by banks. Reserve Bank regulates the interest rates on savings bank accounts and deposits of non-resident Indians (NRI), small loans up to rupees two lakhs, export credits and a few other categories of advances. Through open market operations RBI sells or purchases Government securities. Banks participate in such auctioning as a result money supply is changed leading to changes in rates of interest.

[8] https://cleartax.in/s/slr
[9] https://economictimes.indiatimes.com/definition/statutory-liquidity-ratio

Prudential Norms

Prudential Norms means the ideal/responsible norms to be maintained by the banks. RBI issues "Prudential Norms" to be followed by the commercial banks to strengthen the balance sheets of banks. Some of them are related to income recognition, asset classification and provisioning, capital market exposures. RBI has issued its guidelines under the Basel II for risk management.

Disclosure Norms

One of the important tools for marketing discipline is to maintain public disclosure of relevant information. As per RBI's directives, the banks are required to make disclosures of their annual reports and some other documents about their capital adequacy, asset quality, liquidity, earnings aspects and penalties imposed on them by the regulator.

Anti-Money Laundering Norms

KYC norms (Know Your Customer) Anti-Money Laundering (AML) and Combating Financing of Terrorism (CFT) guidelines are some of the major issues on which RBI keeps issuing its norms and guidelines. Banks and financial institutions (FIs) have been advised to follow certain customer identification procedure for opening of accounts and monitor transactions of suspicious nature for the purpose of reporting the same to appropriate authority. These 'Know Your Customer' (KYC) guidelines have been revisited in the context of the recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT). Detailed guidelines based on the recommendations of FATF and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision (BCBS), with suggestions wherever considered necessary, have been issued. Banks/FIs have been advised to ensure that a proper policy framework on 'Know Your Customer' and Anti-Money Laundering measures is formulated and put in place with the approval of their Boards.[10]

[10] https://rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=9848

Protection of Small Depositors

RBI has set up the Deposit Insurance and Credit Guarantee Corporation (DICGC) to protect the small depositor's interest, in case of bank failure. The DICGC provides insurance cover to all eligible bank depositors up to Rs.1 lakh per depositor per bank.

Para – Banking Activities

Para banking activities are those activities which don't come under the traditional banking activities. Examples of such activities are asset management, mutual funds business, insurance business, merchant banking activities, factoring services, venture capital, card business, and equity participation in venture funds and leasing. The RBI has permitted banks to undertake these activities under the guidelines issued by it periodically.

Annual Onsite Inspection

RBI undertakes annual on-site inspection of banks to assess their financial health and to evaluate their performance in terms of quality of management, capital adequacy, asset quality, earnings, liquidity position as well as internal control systems. Based on the findings of the inspection, banks are assigned supervisory ratings based on the CAMELS rating. Since the RBI is the supervisor of banks, inspecting balance sheets, it knows each bank closely.[11]RBI as a regulator audits books of accounts, NPA accounts of all Banks during Annual Financial Inspection of Head Offices and controlling offices as well as very large branches.

OSMOS

OSMOS refers to Off Site Surveillance and Monitoring System. The RBI requires banks to submit detailed and structured information periodically under OSMOS. On the basis of OSMOS, RBI analyses the health of the banks.[12]

Liquidity Adjustment Facility (LAF)

[11] https://www.indianeconomy.net/splclassroom/how-the-rbi-manages-the-banking-system/
[12] https://www.gktoday.in/gk/how-rbi-regulates-commercial-banks/

Reserve Bank of India's LAF helps banks to adjust their daily liquidity mismatches. LAF has two components – repo (repurchase agreement) and reverse repo. Whenever a bank needs liquidity or financial accommodation, it can use the LAF repo window to get immediate money.

(i) **Repo Rate:** Repo (Repurchase) rate is the rate at which the RBI lends short-term money to the banks against securities. When the repo rate increases borrowing from RBI becomes more expensive. Repo rate is always higher than the reverse repo rate. At present it is 6.00%.RBI's repo rate is the anchor for banks in determining the individual interest rate of banks.

(ii) **Reverse Repo Rate:** It is the exact opposite of repo. In a reverse repo transaction, banks purchase government securities form RBI and lend money to the banking regulator, thus earning interest. Reverse repo rate is the rate at which RBI borrows money from banks. The banks use this tool when they feel that they are stuck with excess funds and are not able to invest anywhere for reasonable returns. At present it is 5.75%.

(iii) **Marginal Standing Facility (MSF):** was introduced by the Reserve Bank of India (RBI) in its Monetary Policy (2011-12). The MSF would be a penal rate for banks and the banks can borrow funds by pledging government securities within the limits of the statutory liquidity ratio SLR.

The scheme has been introduced by RBI for reducing volatility in the overnight lending rates in the inter-bank market and to enable smooth monetary transmission in the financial system. Currently, it is 6.25%.[13]

Market Stabilisation Scheme (MSS)

This instrument was introduced in 2004. Surplus liquidity of a more enduring nature arising from large capital inflows is absorbed through sale of short-dated government securities and treasury bills.

[13] https://learningsessions.in/role-of-rbi-in-indian-banking-system/

The cash so mobilised is held in a separate government account with the Reserve Bank.

Another magnificent service by the RBI to commercial banks is that the central bank settles payments between different banks. This makes the payment transactions between different banks quite easy. The RBI has two facilities called NEFT (National Electronic Fund Transfer) and RTGS (Real Time Gross Settlement) for interbank payment and settlement system.[14]

Other Major Functions of the RBI in the Economy

Issuing Currency-

The RBI has the monopoly of issuing currency of the country. It issues notes of every denomination except one-rupee note and coins and small coins-through the Issue Department of the Bank. The objective of currency issue is merely to give the public adequate quantities of currency notes and coins and that too of good quality.

Banker to the Government-

The RBI acts as the banker to the Government of India and State Governments (except Jammu and Kashmir). As such, it transacts all merchant banking functions for the Governments. The RBI accepts and pays money on behalf of the Government and carries out exchange remittances and other banking operations. As the Government's banker, the RBI provides short-term credit to the Government of India. This short-term credit is obtainable through the sale of the treasury bills. It may be noted that the Central Government is empowered to borrow any amount it likes from the RBI. The RBI also acts as the agent of the Government in respect of membership of the IMF and the World Bank. In addition the RBI also acts as an adviser to Government on almost all economic issues.

Credit Controller-

As the central bank of the country, the RBI has been empowered to formulate, implement and monitor its monetary policy with the vision

[14] https://www.indianeconomy.net/splclassroom/how-the-rbi-manages-the-banking-system/

of maintaining price stability (both internal and external) and ensuring adequate flow of credit to the productive sectors. The RBI controls the total supply of money and bank credit to sub-serve the country's interest. The RBI controls credit to ensure stability in price and exchange rates. To achieve this, the RBI uses all types of credit control instruments quantitative, qualitative, and selective.

Exchange Management and Control-

One of the important central banking functions performed by the RBI is that of maintaining the external value of rupee. The RBI has the authority to enter into foreign exchange transactions both on its own account and on behalf of the Government. The official external reserve of the country consists of monetary gold and foreign assets of the Reserve Bank, besides (Special Drawing Rights or) SDR holdings.[15] India had Foreign Exchange Reserve of around US$ 360bn in December 2018.

Regulator and supervisor of the payment systems-

The RBI Authorises setting up of payment systems, lays down standards for working of the payment system, lays down policies for encouraging the movement from paper-based payment systems to electronic modes of payments, setting up of the regulatory framework of newer payment methods, enhancement of customer convenience in payment systems, Improving security and efficiency in modes of payment.[16]

Collection and Publication of Data-

The RBI has a separate Department of Statistics for collecting, compiling and disseminating statistical information and conducting research related to bank and other financial sectors of the economy including supply of money, credit banking operation and foreign exchange.[17]

Development and Promotions-

[15] http://www.economicsdiscussion.net/reserve-bank/7-major-functions-of-reserve-bank-of-india/6485
[16] https://exampariksha.com/role-functions-rbi-economics-study-material-notes/
[17] https://www.slideshare.net/911995/functions-of-rbi-39648167

The RBI has been aiding development & promoting saving & banking habits. Development of the institutional agriculture & other rural activities has been an area of focus right from its inception.

Clearing house Function-

In India the Reserve Bank of India acts as the clearinghouse for scheduled banks, which have statutory accounts with it. Through this function the Reserve Bank of India enables the banks to settle their transactions among various banks easily and economically.[18]

Recent Changes Introduced by the RBI

The existing guidelines have been revised in such a way that they adhere to the norms of the Insolvency and Bankruptcy Code (IBC) 2016. The new guidelines will help early identification and reporting of stressed assets by banks. As per the new rules, starting 1 March 2018, lenders will have to implement a resolution plan within 180 days for accounts having loans of at least Rs.2000 crores.

RBI has abolished the Joint Lenders' Forum as an institutional mechanism for resolution of stressed accounts and has disbanded existing schemes like Scheme for Sustainable Structuring of Stressed Assets (S4A) which helps strategic and corporate debt restructuring. Secondly, all stressed assets should now be reported to the centralized database of RBI after 30 days of its default. Thirdly, time-bound steps of recognizing bad loans, acting on them, and failing timelines have been notified by the RBI. Fourthly, there will be full disclosure of the borrower now to all lenders. Bigger the borrower, stricter will be the norms and timelines for borrowing.

In addition to this, banks will now have to report defaults of people who have borrowed more than Rs.5 crores on a weekly basis at the close of business on every Friday starting from the week ending 23rd February 2018. All the lenders are also required to submit Central Repository of Information on Large Credits (CRILC) to the RBI every month effective from 1st April 2018.[19]

[18] https://accountlearning.com/central-banking-primary-functions-rbi/
[19] https://qrius.com/role-rbi-regulation-supervision-banks/

CONCLUSION

The Reserve Bank of India by being the apex banking institution of the Country regulates the commercial banks in many ways like acting as the licensor, maintaining CRR and SLR, acting as the banker to the banks, conducting inspection and audits, lending money to the banks, setting repo and reverse repo rates etc. Apart from these functions the RBI also takes steps to avoid money laundering activities, protecting the interest of the depositors. RBI also regulates the money supply in the economy, acts as banker to the government etc. Apart from these traditional functions, the RBI performs various activities of promotional and developmental nature.

SWOT ANALYSIS OF INTERNET BANKING

R. Ajay*

ABSTRACT

Banking sector is the building block of an economy and plays a pivotal role in the financial structure of any nation. It is the most crucial financial intermediary as it connects surplus and deficit economic agents. Moreover, with the advent of technological revolution, the banking today is redefined and re-engineered to provide more sophisticated, innovative and cost-effective products to their customers such as ATMs, tele-banking, Mobile banking, Internet Banking, Core Banking Solutions, Electronic Fund transfers etc. E-banking is an extension of conventional banking system which uses an electronic delivery channel for exchange of banking products and services. With continuous product and process developments evolving rapidly, more products and services may soon become the order of the day. The arrival of computerised technology in Indian Banking scenario dates back to 1990's - the post-reform period. With the adoption of financial sector reforms as suggested by Narasimham Committee, the banking sector has undergone major overhaul and several initiatives have been taken by the Reserve bank of India, the private players and the government to develop e-banking in India. Further, the Government of India enacted the Information Technology Act, 2000 to provide legal recognition to transactions occurring over electronic media and other forms of E-commerce. Following these efforts towards liberalisation, many foreign banks were attracted to India, thereby opening up new markets and innovative products. Today, internet banking has become the essence of the Banks, a strategic tool to transform banking business with a pool of banking services and products accessible 24*7 to customers. This paper aims to analyse the current

* BA., LLB. 2nd year, Government Law College, Dharmapuri, the Tamil Nadu Ambedkar Law University.

scenario of internet banking in India and the major risk areas and challenges faced by banking sector with the usage of Information technology. It also tries to emphasise on the strengths and weaknesses of the internet banking and the future plans that could be adopted to overcome the weaknesses.

Introduction

Financial system in India is dominated by banks, accounting for over 60% of the total assets. Before the implementation of liberalisation, privatisation and globalisation policies by Indian government in 1990's, the banking sector was characterised by lack of competition, low capital base, low productivity and high intermediation cost. There was minimal role of technology and poor quality of service. The thrust of the 1990's reforms was to create an efficient, stable and competitive financial sector by removal of structural bottlenecks, relaxation of restrictions to improve trade, more transparency, creating liquidity and efficient price discovery process, technological upgradation, etc. in order to align the Indian standards with international best practices. Thus, Indian banking sector was exposed to the world market after financial sector reforms in 1991.

Electronic Banking

E-banking can be defined as the automated and effective delivery of new and conventional banking products and services directly to customers through electronic, interactive communication channels. It includes the systems that enable financial institutions, individual customers or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the Internet. It encompasses the wide technological innovations that have taken place in banking from transferring funds online, making online payments for almost any service, managing account balances to making railway, airway and hotel bookings online. It has removed the barriers of 'Brick and mortar' model of banking.

Current Indian Scene: Findings

The Reserve Bank of India has divided the internet banking products in India into 3 categories which are as follows:

- Information System - General purpose information like interest rates, branch location, bank products and their features, loan and deposit calculations are provided in the banks website. No customer identification is done.
- Electronic Information Transfer System - This system entails provision of customer- specific information in the form of account balances, transaction details, and statement of accounts. Customer identification and authentication is required.
- Fully Electronic Transactional System - It allows bi-directional capabilities. Customers can submit transactions for online update. This system requires high degree of security and control. It comprises technology covering computerization, networking and security, inter-bank payment gateway and legal infrastructure.

With around 90 scheduled commercial banks and over 90,000 branches operating in India currently, there are umpteen e-banking products and services which banks have continuously strived to bring for the ease of customers. Some of them have been listed below:

- Automated Teller Machines (ATMs)
- Internet Banking
- Electronic Fund Transfer
- Mobile Banking/ Tele-banking
- Electronic Clearing Services
- Smart Cards
- Door Step Banking
- Electronic Clearing Cards
- Online payments
- NEFT/RTGS
- Electronic Payment Services – E-Cheques

- E-tax
- E-ticketing
- Account Opening Request
- Account statement on emails, etc.

SWOT Analysis

After attempting, the macro level environmental analysis of Indian Banking Industry, a SWOT analysis of e-banking has been done based on the findings.

Strengths:

- It offers superior &user friendly technology
- Anywhere-anytime banking. Further, instant information is available to users as soon as the transaction takes place.
- No paper work and physical handling and storage of paper instruments
- Low cost of online transactions- A Study mentioned that the cost per transaction through a branch was Rs.66, through Automated Teller Machines was Rs.22, and through internet was Rs.10, ignoring the extreme variations owing to the investment cost and nature of transactions.
- Competition from private sector and foreign banks has led to creation of more and more innovative products and services such as e-wallet, plastic cards, online transaction history, buying and selling shares/Mutual funds online, Renewal/premature closure of FD/RD, Bills Payment, Convert to EMI, Online loans, Online tax payments and lots more.
- Faster response to customer queries and complaints. Better customer relationship management.
- Improved management, transparency and accountability.
- Improved trade relations across boundaries with easier transfer of funds through net banking.
- Multi-folds growth in the business of banking sector with variety of banking players in the market- public, private, foreign, regional rural, etc. It also establishes healthy competition and promotes better consumer services.

- With development in technology, banks are reaching more and more remote locations in the country allowing access to rural people who earlier did not have convenient access to banks.
- Strong Regulatory Institutional Framework constituting RBI, IT Act, 2000, Banking Regulation Act, etc.

Weakness

- Complexity in online transactions. The people who are not tech savvy cannot operate bank accounts online unless they are made aware of the e-banking culture.
- There is a 'digital divide' as the poor are excluded from the use of the internet and so from the financial system.
- The confidentiality and integrity of data and information over internet is still a major concern in India. There has been a rise in the number of cyber crimes registered by CBI recently. Of the total cyber crimes recorded in 2012 around the globe, 56% were from India, as per a report of RBI.
- The usage of Internet banking is dependent upon the availability of internet which means when the server is down, the whole system is paralysed.
- Lack of physical presence of bankers which at the time of customer grievances proves to be a negative point.
- Ineffective maintenance of technological infrastructure in some branches.
- Still, some banking personnel are not adequately trained and equipped to handle e-banking which creates barriers and limitations in the system.

Opportunities:

- India is a growing economy with large numbers of investors. It holds immense potential for market expansion.
- One of the biggest opportunities for Indian banking sector is the Indian consumer. With demographic changes over the years, in terms of income levels and rising standards of living, the demand for sophisticated, competitive and retail banking

services have risen. Banks need to tap that market by delivering solutions.

- Integration of domestic banks with foreign markets offers countless opportunities to Indian banking sector to get exposure to the world. In this global world, countries seek high quality banking services with operational efficiency. Hugely talented Indian manpower can seek good opportunities across globe. Additionally, it will create employment opportunities for the youth.

Threats:

- One of the major threats is that it's not secure all the time. Lately, there have been cases where cyber criminals have tricked users through spam sites, social media, etc. to give out their personal information.
- High transaction costs for banks if their customers do not often transact online because huge investment goes into the setting up of Internet banking systems.
- In times of fierce competition if the banks do not upgrade technology in time, they will have to face and suffer losses of customers as well as profits.
- The legal and regulatory framework suffers some loopholes which allow criminals to take advantage of the situation. It needs to be more stringent to prevent frauds.
- Lack of customer loyalty
- Proportion of workforce incapable of handling e-banking business results in inefficiency.

CONCLUSION

E-banking is a survival and growth weapon for businesses and is fundamental aspect of the Indian Banking industry. It has removed all barriers across international borders and created a global banking scenario with ease and availability of services online. The efficient use of technology has facilitated accurate and timely management of the increased transaction volumes of banks which comes with larger customer base. Further, the Information Technology Act, 2000 has

provided the much needed legal recognition to the creation, transmission and retention of electronic data. The upward surge in the ATMs across the nation, multi folds increase in RTGS/NEFT transactions, rise in the number of E-banking users, all are indicative of the fact that Indian banking industry has largely been successful in catering to the needs of the masses and there is no looking back. In spite of such a blessing Internet banking has proven to be, it is hounded by issues like security theft, phishing attacks, money laundering, etc. which is why customers are cautious of conducting banking transactions over the internet. However, such issues can be addressed by ensuring people's awareness in the e-banking code of conduct especially in the rural remote areas. For that, Government can conduct seminars and workshops at grass root level to reach the masses. In addition to that, more funds need to be invested in ensuring safety and security of personal data with installation of customer identification devices, periodic reviews on compliance with laws, information screening techniques, etc. On the whole, we can conclude that technology alone doesn't help but intellectual and trained human resources are supposed to handle such tools which will bring performance improvement and give a competitive edge to banks.

References:

Online reference : http://ssrn.com/abstract=2151162
www.financialexpress.com
www.rbi.org
https://www.shell-livewire.org/business-library/675/swot-analysis-strengths-weaknesses-opportunities-and-threats

OVERREGULATION OF BANKS AND UNDER REGULATION OF NPA: A CAUSE FOR BANK MERGERS IN INDIA

Dr. Fincy Pallissery*
&
Ronak V. Chhabria**

ABSTRACT:

Merger of banks in India is driven by regulatory factors rather than business considerations. In banking sector size is of paramount importance, because it helps in economies of scale and strengthening the capital base of banks. In India, public and private sector banks are leaving for merger due to poor capital reserve ratio. Law enforcement and over regulation by RBI is not improving the competition and capital adequacy of banks, but often leads to forced merger of banking companies. This study will analyze the consequences of over regulation of banks by RBI and identify the reasons as to why it is not leading to strengthening the capital adequacy of banks. Secondly, it studies the need for strengthening banking companies through mergers and maintain competitiveness among banking industry.

Introduction:

Growth of banking companies plays a foremost role in stimulating and stabilizing the growth of an economy[1]. Therefore, failure of banks has a great impact than the failure of firms in other sectors[2]. As a natural corollary, banks are subject to more intense regulation than the other sectors and the state is more pro-active in intervening to prevent bank failures[3]. Banking system in emerging markets have over the past

* Faculty, School of Law, Christ Deemed to be University.
** Fourth Year Law Student, School of Law, Christ Deemed to be University.

[1] Peter Lawrence and Ibotomilongjam, "Financial Liberation in India: Measuring Relative Progress" Kelee Economics Research Paper (KERP 2003/8) Available at www.keele.ac.uk/depts/ec/web/wpapers/kerp0308.pdf

[2] MandarKagade, "Bank Rescue Policies: A comparative Analysis"126 Banking Law Journal 552(2009). Available at http://heinonline.org

[3] *Ibid.,*

decades been transformed by three major trends - privatization, consolidation and the entry of foreign bank on a larger scale[4].

Mergers[5] and Acquisitions of the undertaking[6] is a significant process through which financial service industries accomplish the preferred economic growth. There are many reasons why companies agree to merge[7]. The literature[8] on motives for merger in the banking sector, state the following: cost reduction (economies of scale); rationalization of branch networks; investment for new technologies and processes; income increase, risk reduction due inter alia to diversification, strengthening of the strategic position[9], rapid access to new products or geographic market[10] .

Some of the notable bank mergers in India since 2000, reveals that section 45 of the Banking Regulation Act was used by RBI to

[4] Philip Turner, 'The banking system in emerging markets: How much progress has been made?'(2006) BIS Working Paper (No.28) available at http:/ssrn.org

[5] In the business parlance the expression 'merger' or 'amalgamation' are used interchangeably. Companies Act, 1956 and the earlier companies legislation in India through permitted corporate reorganization, there was no definition or explanation given to the term merger or amalgamation. An explanation for the expression merger is dealt under section 232(8)(i)of the Companies Act,2013. It states two forms of merger (1) Merger by absorption (2) Merger by formation of new companies. Though, title of section 232 is 'Merger and Amalgamation' neither of the expressions is defined.

[6] 'Acquisition' is defined in section 2(b) of the SEBI (Substantial Acquisition of Shares and Takeover) Regulations, 2011.

[7] Introduction to Chapter-II discusses the economic factors underlying bank mergers. It states 'Acquisition means directly or indirectly acquiring or agrees to acquire shares or voting rights in or control over a, target company'. Acquisition of shares of the banking companies is not within the scope this study. But it concentrate on the acquisition of the undertaking of banking companies either voluntarily or by the government order under any of the existing banking legislations.

[8] Dario Focarellietal, "Why do Banks Merge?,"34 Journal of Money, Credit and Banking (2002) 1047-1066 1-21 also in Kalman J. Coben, "The Benefits and Costs of Bank Merger", Journal of Financial and Quantitative Analysis (1966) p.15-57, 120-163.Also bySteven J. Weiss, "Effects of Regulation, Branching and Mergers on Banking Structure and Performance: comments", Southern Economic Journal, Vol.36 (1969) p202-204. 234-237. Also at Darius Palia, "The Managerial, Regulatory and Financial Determinants of Bank Merger Premiums", Vol.41, Journal of Industrial Economics (1993) Pp 91-102. 385-397.Gary G. Gilbert, "Predicting De Novo Expansion in Bank Merger Cases", 29 Journal of Finance (1974) p 151-162. 433-437.Also by Eugene Nelson, "The Merger Movement in Banking 1919-1933", Journal of Economic History, Vol. 45(1985) Pp 285-291. 455-462. Again in A. J. Yeats, "A Frame Work for Evaluating Potential Competition As a Factor in Bank Mergers and Acquisitions: Comment", Journal of Money, Credit and Banking Vol. 6, (1974) Pp 395-402. 465-473.Stijn Claessens, Asli Demirgüç-Kunt, and Harry Huizinga, "How does foreign entry affect domestic banking markets?", Journal of Banking and Finance, 25(5), 891-911 (2000).Robert De Young. Douglas D. Evanoff. Philip Molyneux, "Mergers and Acquisitions of Financial Institutions: A Review of the Post-2000 Literature", J. Financ Serv Res (2009) 36:87-110, DOI 10.1007/s 10693-009-0066-7.

[9] *e.g.* increase of market power resulting from greater market share of merged institutions.

[10] Philippe Gugler, "Causes and Consequences of mergers in banking: The case of UBS" 155 Journal of International Banking Law 1999.Also at Dr.Leela Cejnar and Arlen Durke, "*Competition policy and the banking sector: the need for greater international co-operation*" 583 European Competition Law Review 2013. Available at www.westlaw.org

compel the merger of certain banking companies in order to rescue it from failure[11].

Globalization also has a serious impact on the banking sector. The rising effect on the macro-economic shocks, growing competition among banks and other financial institutions and the general mismanagement of the banks demand that the banks interest need to be protected[12]. Inherent within many merger transactions are bank's desire to obtain "ready-made" branches. Banking offices are obtained through merger either by converting absorbed banks into branches or by transferring acquired branches to absorbing institution[13]. Banks are invaluable to our society. Banking regulation is essential basically for two reasons (1) banks hold large amount of money that is not their own and (2) banks are involved in the risky business of lending money to the borrowers who may or may not return it back. By holding and lending out money, banks impact the economy enormously. Their business strongly impacts public interest through its lending function, which has an inherent level of risk not present in most other businesses[14].

Some economists argue that the process of consolidation is beneficial if it drives out the unproductive banking organizations from the market and if it facilitates increased efficiency in the banking

[11] Major bank mergers between 2000-2015

1. Merger of Times bank with HDFC bank (S.44A of the Banking Regulation Act,1949)
2. Merger Between ICICI LTD. and ICICI BANK (Ss. 391-394 of the Companies Act, 1956)
3. Merger between ICICI Bank and Bank of Madura (S. 44A of the banking Regulation Act)
4. Merger between BANK of Baroda *with* Banaras State BANK (Section 45 of the Banking Regulation Act,1949)
5. PUNJAB NATIONAL BANK AND NEDUNGANDI BANK MERGER (Section 45 of the Banking Regulation Act)
6. Merger between Global Trust Bank and Oriental Bank of Commerce (Section 45 of the Banking Regulation Act, 1949)
7. Merger between BANK of PUNJAB & Centurion Bank (Section 45 of the Banking Regulation Act, 1949)
8. Centurion Bank of Punjab with Lord Krishna Bank (S.45 of the Banking Regulation Act)
9. Merger of IDBI Bank Ltd. With IDBI Ltd (Ss. 391-394 of the companies Act, 1956)
10. Merger of ICICI Bank and the Bank of Rajasthan (S.45 of Banking Regulation Act)
11. Merger between Mahindra Kotak Bank and ING & Vysya Bank (S. 44A of the Banking Regulation Act)

[12] I.L .Vanjaarsveld, "Domestic and International Banking Regulation and Supervision - Defying the Challenges" 119 South African Law Journal 71(2002). Available at http://heinonline.org

[13] Robert H. Marshall, "Legal factors underlying bank mergers" 75 The Banking Law Journal 1958. Available at http://heinonline.org

[14] Peter Lim Felton, *Too Big to manage: A Case for Stricter Bank Merger Regulation*, 52 Santa Clara Law Review 1081(2012) Availableathttp://heinonline.org

companies that survive[15]. Still, a few are of the opinion that mergers among banks reduce bankruptcy risks, because merging two banks creates a bank healthier than their predecessor banks[16]. Ownership structure, regulatory short comings and concern about job losses remain the main obstacles to a faster market driven consolidation process, except in transition economies[17].

Viewing it from the point of systemic risk[18], there are two opinions. On the one hand, bank mergers could stabilize an individual bank as well as decrease systemic risk; because consolidation can lead to increase in the diversification of the company's asset and loan portfolio and consequently higher capital buffers[19]. On the other hand diversification could reduce an institution's individual probability of failure while at the same time making systemic crisis more likely[20].

Several approaches to consolidation are identified. One was the market driven approach, which is common in Central and Eastern Europe and in Latin America. Another is the government driven approach, followed mostly in Asia. In India, RBI is vested with the power over supervision and control over the banks. However, in certain cases the Central government have the decisive voice for bank mergers[21].

Reserve Bank of India is in favour of amalgamation of banking companies[22], provided competition and stability are not compromised[23]. Indian banking industry consists of banks of varied nature. Depending on their nature, there are separate legislations governing those banks in

[15] Robert De Young &Gary Whalen, "Banking Industry consolidation: Efficiency Issues" Working Paper No.110(1994) available at http://ssrn.org

[16] Michael S.H. Shih, " Banking Sector Crisis and Merger as a solution" Available at http://ssrn.org

[17] Gaston Geols and Jorge Rolds, Consolidation and Market structure in Emerging Market banking system'. IMF working Paper (2002) Available http://ssrn.org

[18]Gregor N.F ,Sasha Neumann etal., ' Systemic Risk and Bank Consolidation : International evidence'(2013)Available at http://ssrn.org

[19] *Ibid.,*

[20] *Ibid.,*

[21] For Eg., Acquisition of the undertaking of banks under section 36AE of the Banking Regulation Act,1949

[22]Address by Raghuram Rajan, Governor, Reserve Bank of India on I April,2014. Available at http://articles.economictimes.indiatimes.com/2014-04-01/news/48767599_1_smaller-banks-bigger-banks-merger

[23] Chapter-III discusses the merger routes under the Indian banking laws. It also deals with the number of banks merged in India as on June 2014.

India[24]. Reserve Bank of India regulates 27[25] Public Sector banks[26] including five subsidiaries of State Bank of India and 20 Private Sector Banks[27]. 43[28] foreign banks have their branches in India. In order to meet the credit requirement of rural population, there are 82 Regional Rural banks[29] and many co-operative banks under the supervision of Reserve Bank of India. While talking about the Indian financial institutions and their operating background, it is important to bear in mind that there is multiplicity of the governing statutes applicable to different entities in the Indian credit organizations. Additionally they are governed by the statutory provisions, depending upon the nature of their operations and the form of their organization or ownership[30]. Mergers and acquisitions governing the banks are also not uniform in nature. In some cases, RBI need to sanction the scheme[31], whereas in the compulsory merger under section 45 RBI need to prepare the scheme and the same will be presented before the central government for its sanction. In the case of acquisition of banking companies Central government may after consultation with the RBI acquire such banks and it would prepare the scheme for the acquired banks[32]. For amalgamation between a banking company and NBFC High Court is the sanctioning authority under section 391-394 of the companies Act, 1956. In respect of acquisition of banking companies under the Bank Nationalization Act, 1970 & 1980 central government plays a very important role, though RBI is consulted before placing the same before the parliament. Considering the complex nature of bank merger laws there is a need for study.

Most often, it is the responsibility of the nationalized banks to acquire the undertakings of the failed banks. It creates a burden on these banks to discharge the liabilities created by the transferor banks. However, in the interest of depositors, RBI and central government use the route of merger or acquisition to rescue the failing banks. No doubt,

---

[24] The Banking Regulation Act,1949, State bank of India Act,1955, State bank of India(Subsidiary Banks)Act,1959, Banking companies(Acquisition and transfer of undertakings)Act,1970 &1980

[25] Annexure-II list of Public Sector banks and its Assets and Liabilities from 2012-14

[26] 21 Nationalized Banks, 1 State Bank of India and 5 Subsidiaries of State Bank of India

[27] Annexure-III- List of Private Sector Banks

[28] Annexure-IV –List of Foreign Banks in India

[29] Annexure- V –List of Regional Rural Banks in India

[30] V. Leeladhar, "Consolidation in the Indian Financial Sector" (Speech) 2008. Available at www.rbi.org

[31] Section 44A of the Banking Regulation Act,1949

[32] Section 36 AE read with Section 36AF of the Banking Regulation Act,1949

the depositor's interest will be protected if the failed banks are acquired by nationalized banks or State Bank of India. But in some cases such nationalized banks or State Banks may be able to control the banking industry and that they lead to monopoly at a later stage.

Louis D. Brandles[33] reproduced in his book a speech given by President Wilson; he stated that "The great monopoly in this country is the money monopoly. So long as that exists, our old variety and individual energy of development are out of question. A great industrial nation is controlled by its system of credit. Our system of credit is concentrated. The growth of the nation, therefore, and all our activities are in the hands of few men, who even if their actions are honest and intended for the public interest are necessarily concentrated upon the great undertakings in which their own money is involved…"[34].

Complexities in the regulation of banking sector:

At the fundamental level, the object of bank regulation was designed to wall off banks from market forces[35]. Thus, a protective regulatory regime contributes to the stability in the banking industry. The entry of non-banking financial industry into the banking market is compelling certain banks to acquire such companies and sustain in the market[36]. However, the banking regulations impede such combinations by bringing restrictions for amalgamation or acquisition of banks. All bank mergers occur within a legal context. There is no uniformity in the law governing bank mergers and acquisitions in India. This is due to the multiplicity of banking legalizations due to their varied nature.

Overregulation by RBI- Impact on Behavior of Banking Companies

The Central Board of Reserve Bank of India is empowered under Section 58 of The Reserve Bank of India Act of 1934 to make regulations on a large list of matters. More often than not, this paternalistic power imposes negative externalities on the health of the

[33] Louis D. Brandles,"Other People's Money, and how the bankers use it" Available at http://archive.org/stream/otherpeoplesmone0bran_djvu.txt

[34] *Ibid.,*

[35] Michel Klausner, "An economic analysis of bank regulatory reform: The financial Institutions Safety and Consumer Choice Act of 1991" 69 Washington University Law Quarterly 695(1991)

[36] *Ibid.,*

banking business and the large number of stakeholders, including shareholders, employees, customers and investors. By impositions of stringent regulations, the RBI constrains the autonomy in transactions of banks, and thus there are very limited ways in which the bank can behave in the market.

In a competitive market, the market must have many consumers and bankers, and the goods in question must be largely the same, and firms must have the freedom to enter or exit the market.[37] In a discussion paper on entry of new banks in the private sector,[38] the RBI published that there are 27 public sector banks, 22 private sector banks, 31 foreign banks 86 regional rural banks, 5 local area banks, 1721 urban cooperative banks, 31 state cooperative banks and 371 district central cooperative banks, making up almost 2293 banks in India. As per the data of Office of Registrar General and Census Commissioner, 14,48,23,640 households in India enjoy banking facilities;[39] thus establishing a wide banker and consumer base. Every bank offers goods of similar nature as clear by the definition of 'banking' under Section 5(b) of the Banking Regulation Act of 1949 to include "*accepting, for the purpose of lending or investment, of deposits of money from the public, repayable on demand or otherwise, and withdrawal by cheque, draft, order or otherwise*." If a bank doesn't perform these functions, it is no longer considered a bank.[40] The RBI is committed to ensure free entry to the market.[41] So, ideally banks must perform optimally in this environment, but a significant impact is induced because of the interference of the RBI.

The Guidelines, Regulations, Circulars, Notices and other restrictions issued by the RBI constrain the behavior of the firm. They influence the behavior and performance of the banks in the market significantly. In a competitive market, the bank must ideally be able to perform well. However, the increasing ratio of CRR and SLR that must be maintained with the RBI, the reverse repo rate and repo rate, and

[37] N. GREGORY MANKIW, PRINCIPLES OF ECONOMICS 280 (Cengage 2012).

[38] *Entry of New Banks in the Private Sector- Discussion Paper*, RESERVE BANK OF INDIA (Aug. 10, 2018, 11:22 PM), https://rbidocs.rbi.org.in/rdocs/content/PDFs/FIDIS110810.pdf.

[39] *Number Of Households Availing Banking Services And Number Of Households Having Each Of The Specified Assets*, CENSUS INDIA (Aug. 10, 2018, 11:29 PM), http://www.censusindia.gov.in/2011census/Hlo-series/HH12.html.

[40] *Mahaluxmi Bank v. Registrar of Companies*, AIR 1961 Cal 666.

[41] RAGHURAM G. RAJAN, I DO WHAT I DO: ON REFORM, RHETORIC AND REFORM 42 (Harper Collins 2017).

other ways in which the RBI controls liquidity makes it very difficult for small banks to survive. This forces the banks to either exit the market, or merge with a bigger bank to dilute the effect of these requirements.

An appropriate illustration would be the case of Discontinuation of Letter of Undertaking as a result of the Punjab National Bank case. The RBI issued a Notification[42] discontinuing this service that could be provided by banks. In case a bank has significant amount of revenue being generated due to fee being paid by the customer, the bank is now forced to either exit the market or merge with a larger bank.

Recent tussle between RBI and Central Government

There are sufficient Notices, Guidelines and Regulations by the RBI to establish that there has been heavy regulation of the banking industry. However, the gross NPAs or bad loans of scheduled commercial banks as on December 31, 2017, Rs.6,09,222 crore, accounted for 20.41 per cent of the gross advances.[43] This is a corroboration of non-performance as a result of over regulation. However, this is also of deep concern to the Central Government. In addition to amending the Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002 to include three months imprisonment for non provision of asset details and for the lender to get possession of mortgaged property within 30 days of default, and establishment of six new Debt Recovery Tribunals, the Ministry of Finance issued a notification on 24th July 2018 titled, "Measures to Recover Loan Amount from NPAs."

The major complication is the regulation of Public Sector Banks that are controlled by the central Government. The Reserve Bank of India abolished half a dozen existing loan-restructuring mechanisms in February 2018, and instead provided for a strict 180-day timeline for banks to agree on a resolution plan in case of a default or else refer the

[42] *Discontinuance of Letters of Undertaking (LoUs) and Letters of Comfort (LoCs) for Trade Credits*, RESERVE BANK OF INDIA (Aug. 11, 2018, 12:10 AM), https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI139F15274F2540046CE9C14E9DFEAA60941.PDF.

[43] *Banks' gross NPAs at Rs 8.41 lakh crore in December*, ECONOMIC TIMES (Mar. 9, 2018, 5:56 PM IST) //economictimes.indiatimes.com/articleshow/63234553.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

account for bankruptcy.[44] This brought the Public Sector Banks under the RBI watchlist. It is also clearly shown that the PSBs have more NPAs than Private Banks, and the reasons for this are many, that need to be worked on and addressed by the Government and RBI together. The other significant disagreement was with regard to the interest rates that the RBI refused to reduce.[45]

The RBI and the Government must work together to collectively improve the health of the banking industry. The RBI's independence is crucial for the banking industry. The major suggestion would be to shift the focus of the bank for evaluation before giving out loans to focus on cash flow rather than security. In the long run, the security is very important because it can be used for recovery. However, it involves a lot of transaction and other costs for recovery. A new method for evaluation must be developed.

[44] *RBI's new norms on bad loans wake up call for defaulters: Government*, ECONOMIC TIMES (Feb. 13, 2018, 8::39 PM IST), https://economictimes.indiatimes.com/news/economy/policy/rbis-new-norms-to-speed-up-resolution-of-stressed-assets/articleshow/62901195.cms.

[45] Prabhash K. Dutta, Why the Government and RBI are fighting? ECONOMIC TIMES (Oct. 31, 2018, 09:42 IST), https://economictimes.indiatimes.com/blogs/et-commentary/npa-problem-bankers-alone-should-not-be-blamed/.