VOLUME 15 ISSN 2456-9704

IDENTITY THEFT: A BYPRODUCT OF DYNAMIC TRENDS IN E-BANKING

By Aachal Sah, Apoorva R. Gokare and U Mounika
From Alliance School of Law, Alliance University

Abstract

Internet is one of the most dynamic and growing phenomena, has helped develop a humungous opportunity to enable business and transactions in futuristic and easy means. But, on the contrary, it has also facilitated technologically furthered offenders to commit cybercrimes, one of them being identity theft, where the personal data of any individual is attained illegally, to incur economic advantages. This has crawled into e-banking and has resulted in huge financial losses to the victims as well as banks. The advancement of technology has made things difficult to track the person impersonating, as the internet and online transactions provide a kind of anonymity and privacy to an individual. Although laws are expected to diminish this serious crime, its regulation has been inadequate, incompetence in the imposition of liability for online impersonation and accountability of the offenders. This paper seeks to research the existing legal framework to address the crime of identity theft in e-banking and the complexities faced while imposing liability. It further suggests the passage of Personal Data Protection Bill, 2018, by discussing the result of its implementation, which will enable more security against such heinous crimes. Henceforth, this paper promotes a synergy of law and technology, to curb identity theft in e-banking and provides for effective safeguarding, restricting and resolving mechanisms.

Keywords: *Identity theft, Liability, Data protection laws, E-banking, Cybercrime, Sensitive information.*

Chapter – 1
Introduction

1.1. Background

The Internet has introduced a dynamic environment for businesses and customers to intermingle, which has escalated cheap, interactive and prompt global communications. But, on the darker side, it has also spawned numerous cybercrimes, one of them being identity theft, where the fraudster cannot be traced. Identity theft, in general, refers to "the theft of identity information such as a name, date of birth, social security number, credit card number,"[1] or any other personal identification information to obtain "loans in the victim's name, steal money from the victim's bank accounts, illegally secure professional licenses, drivers licenses, and birth certificates,"[2] or other unauthorized use of the victim's personal information for financial or other activity.[3] The advancement of computer technology and the development of the Internet have provided identity thieves with

[1] Sean B. Hoar, 'Identity Theft: The Crime of the New Millennium' (2001) 80 OLR 1423, 1423.

[2] Martha A. Sabol, 'The Identity Theft and Assumption Deterrence Act of 1998: Do Individual Victims Finally Get Their Day in Court?'(1999) 11 Loy CLR 165, 166.

[3] Michael W. Perl, 'Not Always about the Money: Why the State Identity Theft Laws Fail to Adequately Address Criminal Record Identity Theft' (2003) 94 JCLC 169, 173.

more options to obtain the necessary information to carry out their crime.[4] There are various techniques for procuring personal data from electronic devices such as Hacking, Phishing, Pharming, Skimming, Vishing, etc. Identity theft in e-banking is the appropriation of some individual's personal information to commit fraud for financial benefits. It results in huge financial losses to the victims as well as banks. It is an unintended, but inevitable secondary results of e-banking. Phishing, one of the most popular ways through which identity theft in e-banking is possible, uses false e-mail addresses and false internet sites inciting naive customers to reveal personal information like user ID, passwords, credit card numbers, PIN codes, addresses, bank account numbers, etc.[5] Most often, the false e-mail addresses are similar to the e-mail addresses of the banks in question and they contain a link redirecting the user to false websites, identical to the bank's site.[6] The phisher first 'steals' the identity of the business it is impersonating and then acquires the personal information of the unwitting customers who fall for the impersonation.[7] This has led commentators to refer to phishing as a 'twofold scam' and a 'cybercrime double play'.[8]

Another identity theft variety is related to the use of different types of criminal software, performing actions without the knowledge of the user.[9] It includes "Trojan horse" type viruses, worms or programs of the "keylogger" type, which self-install on the computer of the customer without his knowledge and then capture and record passwords entered by the keyboard, as well as other personal and financial data, and send them to phishing servers.[10] Such criminal acts are labeled by the term "pharming".[11]

Although laws are expected to diminish this serious crime, there has been lacunae in the prevailing laws, inadequacy in its regulation, incompetence in the imposition of liability for online impersonation and accountability of the offenders which have been dealt with in the further chapters.

1.2. Research problem

The paper seeks to research upon identity theft which has been identified as the most prominent cybercrime in e-banking and the legislative framework governing the same, however, several lacunae have to be bridged by adopting laws as well as creating a synchrony between legislations and technology. Hence, our study proposes to research the existing laws, investigating the lacunae and analyze the measures to fill the legislative gaps in India.

1.3. Scope of the study

This study is limited to identity theft in e-banking and does not focus on identity theft in general or any other cyber fraud

1.4. The objective of the study

To study:

- The impact of identity theft in e-banking;

[4] Neal Kumar Katyal, 'Criminal Law in Cyberspace' (2001) 149 University of Pennsylvania Law Review 1003.
[5] Silvia Parusheva,'Identity Theft and Internet Banking Protection' (2009) Economic Alternatives 44, 44.
[6] ibid.
[7] Vikrant Narayan Vasudeva, 'Phishing: Deception in Cyberspace' (2010) 12,12.
[8] Robert Stevenson, 'Plugging the "Phishing" Hole: Legislation v. Technology', (2005) Duke L & T Review 1, 3.
[9] Silvia Parusheva, 'Identity Theft and Internet Banking Protection' (2009) Economic Alternatives 44, 44.
[10] ibid.
[11] ibid.

- Legislative measures to curb identity theft in e-banking;
- Allocation of liability;
- Effectiveness of Data Protection Laws to safeguard e-banking customers.

1.5. Review of literature

Jennifer Lynch, "Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks", *Berkeley Technology Law Journal*, Vol. 20, No. 1, 2005, pp. 259-300.

This article discusses the growing identity theft problem in cyberspace, focusing specifically on phishing attacks. It is divided into three parts where Part I provides an overview of identity theft, Part II provides facts and statistics on the phishing problem and Part III discusses recent developments in fighting identity theft. It concludes by demonstrating that no single crime control method alone will be enough to combat phishing. Only a combined approach, incorporating strategies from each level, will diminish the problem.

Keith B. Anderson, Erik Durbin and Michael A. Salinger, "Identity Theft", *The Journal of Economic Perspectives*, Vol. 22, No. 2, 2008, pp. 171-192.

This article highlights how big the problem of identity theft is, which is made possible by the nature of modern payment systems, as sellers are willing to offer goods and services to strangers in exchange for a consideration. Thus, the paper also addresses the challenge to formulate policies that strike the right balance between allowing access to information by people who have a legitimate use for it and providing incentives to exercise care to prevent abuse.

Mark T. Gillett, Obrea O. Poindexter, Veronica McGregor and Martin Villongco, "Developments in Cyberbanking", *The Business Lawyer*, Vol. 59, No. 3, 2004, pp. 1335- 1345.

This article discusses the increased security concerns for financial institutions and further goes on to elaborate on the concept of "phishing". While addressing the concerns of security, it provides for measures for detection, prevention and response steps in assisting the issue of phishing. It further talks about risks inherent in financial web-linking, compliance risks to be considered when allowing another website to create a link to the website of the financial institutions for completion of transactions.

BR Sharma, *Bank Frauds Prevention & Detection*, Universal Law Publishing Co Ltd., India, 2004.

This book is a remarkable contribution to understanding the concept of bank fraud. It is a multi-professional monograph, written in non-technical language, addressed to all those who are concerned with and have to deal with bank frauds. It talks about Bank Fraud Spectrum, Bank Frauds Prevention, Fraud Prevention Strategies, etc. which gives us an insight into identity theft in e-banking and, various measures which can be taken to handle e-banking frauds.

Dr. Deepti P. Lele, Dr. Shraddha Purandare, "Cyber Crimes as a Growing Menace", *International Journal of Informative and Futuristic Research*, Vol. 5, No. 3 (2017).

The paper discusses how identity theft has emerged as the crime of the millennium and how such theft is committed. It further throws light on the legislative provisions governing identity theft in India and the impact of such acts on the consumer base and efficient ways

to prevent such future incidences.

T.R. Hema Monisha, M.S. AswathyRajan, "An Analytical Study on Offences under IT Act with Special Reference to Section 66", *International Journal of Pure and Applied Mathematics*, Vol. 119, No. 17 (2018), pp. 1571-1588.

The Article addresses the legislative framework under the Information Technology Act, 2000 in Sections 66A-66F. The paper also addresses the insufficiency of the law governing cybercrimes and a casewise analysis of such crimes.

Keith B. Anderson, "Who Are the Victims of Identity Theft? The Effect of Demographics", *Journal of Public Policy & Marketing*, Vol. 25, No. 2, 2006, pp. 160-171. This article is concerned with educating consumers about limiting identity theft risk. It uses the Federal Trade Commission's 2003 identity theft survey data and examines the relationship between a person's demographic characteristics and the likelihood of experiencing identity theft. Among other factors, the risk of identity theft appears to be higher for people with higher incomes, for younger consumers, and women.

1.6. Research questions and Hypothesis

1) Are the prevailing laws adequate to curtail the current issue of identity theft in e-banking?
2) What are the complexities of imposing liability for identity theft?
3) Whether data protection laws can provide for an effective security framework?

The study will be based on the hypothesis that the laws which deal with identity theft are not well equipped to curb the problem of identity theft.

1.7. Research Methodology

The methodology adopted in this paper is doctrinal research, wherein extensive interpretation of available literature has been done whereby this paper would suggest measures to curb the problem of identity theft in e-banking.

Chapter – 2
Prevailing Legislations concerning Identity Theft in India and Their Lacunae

The Model Law on e-commerce and e-governance was enacted by the United Nations Commission on International Trade Law (UNCITRAL) in 1997. The enforcement of the Model Law was done by countries around the world and India became the 12th nation in the world to have enacted exclusive legislation on Information Technology based on UNCITRAL Model Law.[12] Having erected a framework for comparative scrutiny of the Information Technology Act, 2000 with cybercrime legislative standards across the world, it is visible that the IT (Amendment) Act, 2008 was introduced to tackle unresolved cyberspace issues such as internet fraud, pornography, data theft, phishing, etc., that were not explicitly covered under the old legislation but are at the heart of internet activity, nevertheless.[13] Hence, this chapter shall delve upon the legal framework regarding identity theft in India and whether the prevailing laws are adequate to curtail the current issue of identity theft in e-banking.

2.1. Legal framework regarding identity theft in India

[12] Dr. Swapnil Sudhir Bangali and Dr. Harita Swapnil Bangali, 'In-Built Challenges for Information Technology Law in India' (2016) 4 International Journal of Advanced Research 652, 652.

[13] Amlan Mohanty, 'New Crimes Under the Information Technology (Amendment) Act' (2011) 7 IJLT 105, 109.

2.1.1. Information Technology Act, 2000

Before its amendment in 2008, Section 66 of the Act only addressed hacking as a cybercrime wherein some deletion, destruction, reduction or alteration in the value of computer resources attracted penal sanctions and identity theft was not addressed separately, but it fell within the ambit of hacking. If a person obtained personal information from the computer in a secretive manner without causing any changes in it whatsoever, this provision could not be used. However, the term identity theft itself was used for the first time in the amended version of the IT Act. Section 66 was broadened in scope and included any person who dishonestly or fraudulently, does any act referred to in Section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.[14]

Section 66A[15] which is now held to be unconstitutional by the Supreme Court in the landmark judgment of *Shreya Singhal v. Union of India*,[16] on account of it being violative of Fundamental Right of freedom of speech and expression, covered the crimes of Phishing.

Section 66B provides for dishonestly receiving stolen computer resource or communication device.[17]

Section 66C provides punishment for identity theft. Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to be fine may extend to rupees one lakh.[18] It makes identity theft as a standalone crime. This section also covers password theft and the offense of phishing.[19]

Section 66D provides punishment for cheating by personation by using computer resource. Whoever, utilizing any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.[20]

Hence, the aforementioned laws can be applied for punishing the offender depending upon the method using which identity theft has been committed. Though provisions of the I.T Act delves upon identity theft in general, it is pertinent to note that identity theft in e-banking shall also be governed by the same provision.

The enactment of the I.T Act brought in amendments in various other statutes, one of them being the Indian Penal Code, 1860. Since identity theft involves forgery, certain provisions of IPC like forgery,[21] forgery for purpose of cheating,[22] reputation,[23] using as genuine a forged document,[24] and possession of a document known to be forged and

[14] Information Technology Amendment Act 2008, s 66.
[15] Information Technology Amendment Act 2008, s 66 A.
[16] *Shreya Singhal v. Union of India* (AIR 2015 SC 1523).
[17] Information Technology Amendment Act 2008, s 66 B.
[18] Information Technology Amendment Act 2008, s 66 C.
[19] Ms. Preeti Jain, 'Cyber Crimes- An Indian Perspective'(2016) Bharati Law Review 183, 194.
[20] Information Technology Amendment Act 2008, s 66 D.
[21] Indian Penal Code 1860, s 464.
[22] Indian Penal Code 1860, s 468.
[23] Indian Penal Code 1860, s 469.
[24] Indian Penal Code 1860, s 471.

intending to use it as genuine,[25] etc. were amended by the I.T Act to include electronic records thereby widening its scope to include computer data crimes as well.

2.1.2 Reserve Bank of India Notification on Customer Protection - Limiting Liability of Customers in Unauthorized Electronic Banking Transactions

The Reserve Bank of India (RBI), in its annual report 2017-2018, has made it clear as to who will bear the financial liability in case of an unauthorized electronic banking transaction.[26] A framework has been established on limiting the liability of such bank customers depending upon whose fault or negligence it is in the case and accordingly, the loss will be borne either by the customer or bank. If neither customer nor bank is at fault and the fault lies within the system, the customer's liability will be zero if he or she reports it to the bank within 3 working days of receiving the communication from the bank about the unauthorized transaction.[27] If a customer reports it with a delay of 4-7 working days then the maximum liability of the customer ranges from ₹ 5,000 to ₹ 25,000, depending on the type of account.[28] In case there is a delay of more than 7 working days in reporting the transaction, customers' liability will depend on the bank's policy.[29]

2.2. Inadequacy of laws in India to deal with identity theft

There is no specific law for the regulation of online data in India. A bill named Draft Personal Data Protection Bill, 2018 is under deliberation in the Parliament and has not been passed yet. However, the Information Technology Act, 2000 after its amendment in 2008, along with the I.T Rules of 2011 has succeeded in laying down the framework of regulations in cyberspace and misuse of personal data can be protected to some extent by providing criminal and civil relief for misuse of data[30] to a large extent. It is a generic piece of legislation dealing with various issues like digital signatures, public key infrastructure, e-governance, cyber contraventions, cyber offenses, confidentiality, and privacy.[31]

Nevertheless, the prevailing laws are inadequate to curtail the current issue of identity theft and need to be discussed. With the development of e-banking, various security risks have come to the forefront. Computers today are being misused for illegal activities like e-mail espionage, credit card fraud, spams, and software piracy and so on, which invade our privacy and offend our senses.[32] In the U.S. alone, about 15 Million

[25] Indian Penal Code 1860, s 474.

[26] Nikhil Agarwal, 'RBI fixes liability if your bank account is hacked' (*Livemint*, 29 August 2018) <https://www.livemint.com/Companies/mBxEdGgNeEPTZAOMmYL1nI/RBI-fixes-liability-if-your-bank-account-is-hacked.html> (accessed 22 December 2019).

[27] ibid.

[28] ibid.

[29] Reserve Bank of India, *Customer Protection - Limiting Liability of Customers of Co-operative Banks in Unauthorized Electronic Banking Transactions*, RBI/2017-18/109 DCBR.BPD.(PCB/RCB).Cir.No.06/12.05.001 /2017-18.

[30] Faisal Fasih, 'Regulation of Data in The Cyberspace- Drawing Roadmap for India' (2011-2012) 2 CNLU 100,100.

[31] ibid 102.

[32] Jaro Jasmine and Aswathy Rajan, 'A Critical Study on Concept of E-Banking and Various Challenges of IT in India with Special Reference to RBI"S Role in

residents have their identities used fraudulently every year, with a total loss of about $50 Billion.[33] Similarly in India, as per the research finding of a company, one out of four is a victim of identity theft and such cases have risen by 13% since 2011.[34] As per Microsoft's Third Annual Computing Safer Index, at least 20% of Indians have fallen prey to phishing attacks and identity theft has caused a loss of around Rs. 7500 on an average.[35] The numbers shown in this Survey is quite large if we consider the fact that the total internet users in India are around 19.9% of the entire population and all these are being caused due to the lacunae in the prevailing law.[36] Thus, arises the need to fill in such lacunae with stronger legal provisions which will provide for an effective regime to curb identity theft in e-banking where the stolen identity of the victim can be used to cause economic loss to the victim of such theft.

While Section 66C deals with deceitful use of passwords, electronic signatures and the like, section 66D involves the use of a "communication device" or "computer resource" as a means of impersonation, which in effect, entails the use of computers, cell phones for fraudulent purposes. While the former provision includes intangible but unique identifiers and symbols attached to individuals, the latter envisages instances where the offender has physical access to someone else's devices.[37] However, in the absence of a clear definition of "Unique identification feature" and the advent of new forms of cybercrime such as SMS spoofing,[38] there may exist grey areas relating to identity theft such as misuse of cell phone numbers, which, in the strict sense, may not be consistent with the idea of a "unique" identification feature of an individual, and not fitting the definition of "computer resource" or "communication device" under section 2(1)(K) and (ha) respectively, may lie outside the scope of both, section 66C and 66D, which is a serious concern for cybercrime officials.[39] Under section 66C, the fine provided for identity theft may extend up to only rupees one lakh i.e., a minimal token fine with an upper limit has been prescribed in the Act. There should be different degrees of punishment based on the nature of the crime committed after the identity theft taking place, a provision that could have been transplanted into the Indian legislation to make it more comprehensive, instead of having a uniform punishment of three years for the crime of

Safe Banking Practices' (2018) 119 International Journal of Pure and Applied Mathematics 1661, 1666.

[33] Rob Douglas, 'Identity Theft Statistics: 15 million victims a year' <www.identitytheft.info/victims.aspx> accessed 20 September 2019.

[34] Silicon India, 'Identity Theft: a Major Threat to India' (2013) <www.siliconindia.com/finance/news/Identity- Theft-a-Major-Threat-to-India-nid-143825.html> accessed 21 September 2019.

[35] Microsoft, 'Identity theft costs Indians Rs 7,500 on an average: Microsoft' *Timesofindia-economic times*, (India, 11 Feb 2014) <http://articles.economictimes.indiatimes.com/2014-02-11/news/47235749_1_identity-theft-micr osoft-newinternet-users> accessed 22 September 2019.

[36] Internetlivestats.com, 'India Internet Users-Internet Live Stats (2015) <www.internetlivestats.com/internet- users/india/> accessed 21 September 2019.

[37] Amlan Mohanty, 'New Crimes Under the Information Technology (Amendment) Act' (2011) 7 IJLT 104, 113.

[38] Vineeta Pandey, 'Cell Abuse: SMS Spoofing's Forgery' *The Times of India* (India, 18 July 2004) <https:// timesofindia.indiatimes.com/india/Cell-abuse-SMS-spoofings-forgery/articleshow/782197.cms> accessed 18 Sep 2019.

[39] Amlan Mohanty, 'New Crimes Under the Information Technology (Amendment) Act' (2011) 7 IJLT 104, 114.

identity theft.[40] It may also depend on the value of goods or money accumulated over a while as a result of the identity theft[41] and may also vary based on the number of identifying markers stolen.[42]

Although according to section 75(2), this Act shall apply to an offense or contravention committed outside India by any person if the act or conduct constituting the offense or contravention involves a computer, computer system or computer network located in India,[43] but the jurisdictional issues still cannot be resolved. The tracking and prosecution of identity thieves who operate in a multi-jurisdictional environment are difficult and problematic. When the accused is a non-Indian citizen, the country of his citizenship has dissimilar laws about identity theft and has not signed an extradition treaty with India, the arrest of such an accused cannot be undertaken.[44]

Apart from the IT Amendment Act, being the caretaker of the Indian banking sector, RBI has the due responsibility in establishing its strong and effective control over all the banks in India to provide the citizens of this land with a transparent banking system[45] which resulted in RBI's notification on Customer Protection - Limiting Liability of Customers in Unauthorised Electronic Banking Transactions but there has been no proper implementation of the same.

The increased use of the internet for financial transactions has facilitated the work of identity thieves while tracking has become much more difficult or sometimes impossible. Identity theft in e-banking has an impact on the personal finances and emotional well-being of victims, and on the financial institutions and economies of countries.[46] It presents challenges for law enforcement agencies in India as well as governments worldwide.[47] This paper reveals that identity theft is a growing and evolving problem that requires a multi-faceted and multidisciplinary approach by law enforcement agencies, financial institutions, and individuals. It is further advocated in the next chapters that apart from the need to fill in such lacunae with stronger legal provisions, financial institutions should take measures to protect personal information better and that individuals should be educated about their rights, and be vigilant and protect their personal information in cyberspace.

Chapter - 3
Complexities in Allocation of Liability

The menace of identity theft has pervaded all

[40] Identity Theft and Assumption Deterrence Act 1998, s 1028.
[41] Identity Theft and Assumption Deterrence Act 1998, s 1028 (b)(3)(A).
[42] Identity Theft and Assumption Deterrence Act 1998, s 1028 (b)(3)(4).
[43] Information Technology Amendment Act 2008, s 75.
[44] Aishwarya Joshi, 'Identity Theft- A Critical and Comparative Analysis of Various Laws in India' 2 Journal on Contemporary Issues of Law 1, 14.
[45] Akshay Ramesh and Gokul L, 'India: Present Status of Consumer Protection in Indian Banking Sector' (*Mondaq* 19 November 2019) < http://www.mondaq.com/india/x/865580/Dodd-Frank+Wall+Street+Reform+Consumer+Protection+Act/Present+Status+Of+Consumer+Protection+In+Indian+Banking+Sector> (accessed 22 December 2019).
[46] F Cassim, 'Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?' (2015) 18 PELJ 69, 69.
[47] ibid.

societies. The rapidity and anonymity of the internet have escalated the problem of detection. It has been mooted that any legislation which seeks to punish internet-related offenses or crimes needs to overcome three hurdles: the difficulty inherent in finding the perpetrator of an online crime, obtaining personal jurisdiction and enforcing the judgment.[48] Thus, the major trouble is to find the perpetrator, where the risk of him getting caught is very low. The e-thief's sites are generally not active for more than 54 hours, so the spoofed site will disappear before law enforcement has even received workable information on the theft.[49] Besides, although a perpetrator's server information is revealed during the spoof, catching phishers is still difficult because they use multiple IPs, redirect services, and hijacked third-party computers located in remote places of the world.[50]

The sophistication of computer attacks along with the complexities of the modern computer age has made it difficult to trace the offender in case of identity theft. Thus, imposing liability only on the banks or the customers itself is not appropriate, where the e-thief gets away with his crime. Law enforcement doesn't have all the necessary resources to attend to identity theft, which are costly to investigate and prosecute. They have to conquer jurisdictional issues, which are the most difficult ones as anyone sitting in any corner of the world can be involved in the identity theft of an individual. Instead of increasing resources and training for law enforcement, legislators have chosen to focus on stiffer penalties by trying to pass more specialized laws.[51]

The Protection of Personal Information Act, 2013, is a legislation in South Africa enacted to protect the personal information processed by private and public bodies, which provides for the protection of the rights of persons regarding unsolicited electronic communication.[52] This Act places liability on financial institutions to handle the personal information of its clients with the utmost care and responsibility, and provides penalties for its non-compliance or if made available for cloning, which may extend up to R 10 million or imprisonment of up to 10 years.[53]

Identity Theft Penalty Enhancement Act, 2004, a legislation in the United States of America, aimed at imposing tougher penalties on the offender of aggravated identity theft. Following this legislation, another Act came into existence in the US, called Identity Theft Enforcement and Restitution Act, 2008, which aimed at enhancing the identity theft laws. This Act applied to online identity theft too. The effect that this sought to achieve was not fulfilled as the perpetrator was almost impossible to trace. Escalating the imprisonment wouldn't even deter the criminal in committing identity theft. Thus,

[48] Stevenson 'Plugging the 'phishing' hole: legislation versus technology' (2005) 5 *Duke Law and Technology Review*, Vol. 5 (2005).

[49] Internet Fraud Complaint Center, *'Spoofed E-mails & Websites – A Gateway to Identity Theft and Credit Card Fraud'*, 2 (2002), at http://www1.ifccfbi.gov/strategy/63003SpoofNote.pdf .

[50] Press Release, U. S. Department of Justice, Operation Web Snare 8 (26 Aug, 2004).

[51] Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. Rev. 1003, 1011 (2001).

[52] Cassim Fawzia. "Addressing the Spectre of Phishing: Are Adequate Measures in Place to Protect Victims of Phishing?" *The Comparative and International Law Journal of Southern Africa*, Vol. 47, No. 3 (2014).

[53] Section 19, The Protection of Personal Information Act, 2013.

tougher sentencing laws would only induce 'false guilty pleas' by innocent defendants who do not want to risk trial.[54]

In most cases, banks compensate their clients for losses incurred as a result of the identity theft through phishing scheme when there is no negligence of the client.[55] But there arises a question, whether there should be compensation for the victim's time and effort in dealing with identity theft. Some companies or financial institutions do not even report a crime of identity theft to avoid diminution in public trust and to avoid a reduction in their share pricings. Such acts of the banks should also be curbed by imposing higher penalties.

3.1. Synchrony of Law and Technology

As Nobles say, "Prevention is always better than cure", creating awareness and taking precautions to safeguard personal information by banks as well as customers, is a better way than imposing liability on banks, even when it's not their fault. Therefore, the focus should be on the technological changes with legislations playing a supporting role. Only technology can combat technology. Financial institutions maintain their websites, through web-linking, where payment and other transaction facilities available for their customers are directed to other websites, which might not be handled by the financial institutions itself. This increases the risk of data leakage if the third party website doesn't adhere to compliances.

Also, there is a high risk that there might be sites with similar internet addresses that replicate the genuine look of bank sites. To mention as an example, www.citibank.com opens to the Citibank website, but then www.citbank.com, which is very similar to the original one but doesn't have a second 'i', takes anyone to a website which promises an assortment of services, like mortgages, credit cards, and other financial utilities.[56] The services rendered are quite similar to that of Citibank, it doesn't even make an effort to clarify that it is not the Citibank's website. There are very high chances that financial institutions' names can be mistyped, leading the consumers to be directed to websites with either a similar or deliberately visually identical domain.[57] This might deceptively lead to situations where customers transfer their personal information to fraudulent websites. As obtaining a domain is a cakewalk in this era, banks must be heedful in supervising their domain names.

"It's a good news when everyone works together, they can really catch the crooks. The bad news is that the criminals are like cockroaches – you kill one and 20 pop-up".[58] The real problem is a lack of resources and incentives than a lack of laws. It can be seen that it is not possible to impose liability on an entity at one level. Participants at every level must put in greater efforts to inculcate new practices to inhibit the crime of identity theft.

---

[54] Jennifer Lynch,. "Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks." *Berkeley Technology Law Journal*, Vol. 20, No. 1 (2005).

[55] Reserve Bank of India, *Customer Protection - Limiting Liability of Customers of Co-operative Banks in Unauthorized Electronic Banking Transactions*, RBI/2017-18/109 DCBR.BPD.(PCB/RCB).Cir.No.06/12.05.001 /2017-18.

[56] Mark T Gillett, Obrea O Pindexter, Veronica McGregor and Martin Villongco, "Developments in Cyberbanking" (2004) 59 BUS LAW 1335.

[57] ibid.

[58] Avivah Litan, The War on ID Theft, Red Herring, Oct 29, 2004, <http://www.redherring.com/Article.aspx?a=10938&sector=Industries&subsector=SecurityAndDefense> accessed on 10 October 2019.

eBay's VP for Security noted – "Technology can solve 60 percent of the problem . . . [e]ducation and awareness can solve 20 percent, and no matter how good the industry is, there will be people who fall, victims, so 20 percent will have to be handled by law enforcement".[59]

The crime of identity theft is an evolving and escalating problem that can be combated with a multi-faceted and multi-disciplinary approach. The Information Technology Act, 2000 and the regulations given by Reserve Bank of India show that the State is making efforts to lower such crime rates, but unfortunately, haven't been able to succeed to a great extent. The Information Technology Amendment Act, 2008, allows authorized agencies broad reactive access to personal information held by the private sector for investigation purposes.[60] However, the Indian government's access to and disclosure of private sector data has been criticized because it does not adopt principles of natural justice and its practices are susceptible to corruption and collusion.[61] The challenge here is to devise guidelines that strike a balance permitting reasonable admission of information to people who have legitimate use of such information, and simultaneously provide a shield to individuals.

Financial institutions have to adopt improved technological measures that align with the prevailing technological environment. Such measures include the introduction of a biometric system for online transactions like iris scan, fingerprint and hand imaging for identification of individuals. Transactions should be made fool-proof with the assistance of the above-mentioned measures and verified by both the bank and the customer.

Incentives must be provided to those bearing the loss so that they abandon less efficient mechanisms. The most logical candidates for the same are banks and financial institutions, who are more familiar with the industry and will be able to create new systems to prevent identity fraud. The goal is to provide those, who have the greatest power to prevent identity theft and the most knowledgeable about the systems for granting credit, the incentive to thwart identity theft and allow them to come up with solutions to the said problem. If they cannot create such a solution, then they will bear the losses generated by identity theft.

Chapter – 4
Role of Data Protection Laws in Curbing Identity Theft in E-Banking in India

Data protection laws generally refer to the mechanisms adopted by the legislation to minimize the intrusion caused by the usage of personal information without the consent of the data principals. It is observed that not only is such data theft done by private entities, even the government entities are aboard in such intrusions,[62] and the irony being these entities are known as data fiduciaries.[63]

[59] Saul Hansell, *Online Swindlers, Called "Phishers", Lure the Unwary*, N.Y. Times (24 March, 2004).

[60] Abraham S and Hickok E, "Government Access to Private-Sector Data in India" (2012) IDPL, 302,305.

[61] ibid. 302, 315.

[62] Suneeth Katarki, Namita Vishwanath, Ivana Chatterjee, India: The Personal Data Protection Bill, 2018-Key Features and Implications, (Mondaq, 15 August 2018) <http://www.mondaq.com/india/x/727550/data+protection/The+Personal+Data+Protection+Bill+2018+Key+Features+And+Implications> accessed on 12 September 2019.

[63] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy Protecting Privacy, Empowering Indians (2018)

Hence, this chapter shall delve upon how data protection law, which is to be enacted in India can prevent identity theft.

4.1. Role of Draft Personal Data Protection Bill, 2018, in curbing Identity theft in e-banking.

The Justice B.N. Srikrishna Committee Report on "Free and Fair Digital Economy, Protecting Privacy and Empowering Indians"[64] and the Draft Personal Data Protection Bill, 2018 threw light on the importance of data protection in India and the need for a legal framework to protect the personal data of individuals. The foundation of the bill i.e., the Right to Privacy has been inherited from the landmark judgment of the Supreme Court in the case of *Justice K.S. Puttuswamy (Retd.) &Anr. v. Union of India &Ors.*,[65] wherein the right to privacy was upheld as a fundamental right under Article 21 of the Constitution of India.

4.2. Foundation of the Draft Personal Data Protection Bill, 2018

The Bill if enacted shall apply to any bank collecting, disclosing, sharing or otherwise processing personal data within the territory[66] or any person or body of persons incorporated or created under Indian law[67] shall fall within the purview of the Bill. The Bill shall also apply to the Banks which are situated out of India but are processing personal data in connection with

any Indian citizen, business carried on in India or any systematic activity of offering goods or services to such data principals within the territory of India[68] or in connection with any activity which involves profiling of data principals within the territory of India.[69] The major definitions that need to be considered when dealing with identity theft in e-banking are that of Personal Data,[70] Personal Data Breach[71] and Financial Data.[72]

Upon analysis of the above definitions, it can be ascertained that identity theft is brought under the purview of the bill, as it delves upon unauthorized use, alteration or destruction which shall compromise confidentiality or integrity of the personal data i.e. any attribute that can identify an individual, to a data principal.[73] It also deals with personal data to identify any account or card or payment instrument issued by a financial institution.[74] Hence, formulating a legal framework for the governance of identity theft in e-banking. It is eminent to also note that certain data has been classified as Sensitive Personal Information such as financial data and official identifiers which is the data generally possessed by

<https://www.prsindia.org/sites/default/files/bill_files/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill%2C%202018.pdf> accessed on 14 October 2019.

[64] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy Protecting Privacy, Empowering Indians (2018) <https://www.prsindia.org/sites/default/files/bill_files/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill%2C%202018.pdf> accessed on 25 September 2019.

[65] *Justice K.S. Puttuswamy (Retd.) & Anr. v. Union of India & Ors.* W.P. (Civil) No. 494 of 2012.

[66] Draft Personal Data Protection Bill, 2018 s 2(2)(a).

[67] Draft Personal Data Protection Bill, 2018 s 2 (1)(b).

[68] Draft Personal Data Protection Bill, 2018 s 2(2)(a).

[69] Draft Personal Data Protection Bill, 2018 s 2(2)(b).

[70] Draft Personal Data Protection Bill, 2018 s 2(29).

[71] Draft Personal Data Protection Bill, 2018 s 2(30).

[72] Draft Personal Data Protection Bill, 2018 s 2(19).

[73] Draft Personal Data Protection Bill, 2018 s 2(30).

[74] Draft Personal Data Protection Bill, 2018 s 2(19).

banks, hence, requiring data fiduciaries and data processors, collecting or processing such sensitive data to provide additional security mechanisms to protect such data.

4.3. Consent based nature of the Bill

Few of the prominent features to be considered by data fiduciaries while collecting or processing data should be analyzed for data fiduciaries to prevent identity theft in e-banking. It is to be taken into consideration that the Bill is entirely consent-based, which is to be expressly provided and, without the consent of the data principal no data can be collected by the banks, also such consent can be withdrawn at any point of time.[75] It is also eminent to note that, such consent should be given no later than the processing of such data explicitly.[76] In the case of sensitive private data, explicit consent has to be obtained for different purposes of processing data.[77] Also, the banks cannot collect such personal data that is not required to provide banking services.[78] However, when a data principal withdraws such consent he shall bear the consequences of such withdrawal.[79] Concerning consent, it is pertinent to note that as compared to the General Data Protection Regulations,[80] the exemption of contractual relationships has been omitted from the bill to protect the severability of consents under a contract and prevent Data Fiduciaries from bundling unrelated data processing activities in contracts.[81]

4.4. Fairness and transparency

Another prominent provision in Bill deals with the mandate of notice to be provided by Data fiduciaries and, in this case, the banks. The banks are to provide fair and transparent notice to the data principals while collecting their data describing the collection, use, access, storage, disclosure, the security of the personal data along with the choice and their rights. This should be applied for both online and offline collection modes.[82]

4.5. Liability upon data fiduciaries

The New Bill also allocates the liability upon data fiduciaries in case of breach of personal data. It was entailed upon the data fiduciaries an exemplary civil punishment[83] which, shall pressurize banks to improve security measures to prevent identity theft. The Bill also provides for criminal punishment of 3-5 years imprisonment for data fiduciaries who knowingly, intentionally, or recklessly obtain, disclose, transfer or sell Personal Data or Sensitive Personal Data provided that such acts result in harm to a Data Principal.[84]

Thus, the Draft Personal Data Protection Bill is a welcome move to curb identity theft in e-banking and shall be an effective mechanism. Though the Draft Bill may not be 100% perfect at this stage and might need several amendments in the future it is high time India has a Data Protection Bill which shall be

[75] Draft Personal Data Protection Bill, 2018 s 12(2).
[76] Draft Personal Data Protection Bill, 2018 s 12(1).
[77] Draft Personal Data Protection Bill, 2018 s 18(2).
[78] Draft Personal Data Protection Bill, 2018 s 12(3).
[79] Draft Personal Data Protection Bill, 2018 s 12(5).
[80] General Data Protection Regulation 2016/679.
[81] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, A Free and Fair Digital Economy Protecting Privacy, Empowering Indians (2018) <https://www.prsindia.org/sites/default/files/bill_files/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill%2C%202018.pdf> accessed on 27 October 2019.
[82] Draft Personal Data Protection Bill, 2018, s 8.
[83] Draft Personal Data Protection Bill, 2018, s 69(2).
[84] Draft Personal Data Protection Bill, 2018, ss 90, 91.

perfected over time. But in the face of several data and identity thefts and no legislation to cover it, there is a dire need for the Bill to come into effect. Hence, if this legislation comes into force it shall safeguard the victims from identity theft.

Chapter-5

Conclusion

Identity theft in e-banking as discussed being a major issue without an effective legislative framework preventing it is the concern of the hour as various mechanisms are being developed by i-thieves to attain personal identities which shall enable them to get the benefits of the persons' financial accounts with the banks. As technology is developing the mechanisms have become quite innovative and the lack of law about the matter of identity theft has been a major bane in India.

The Information Technology Act, 2000 only provides for punishment in case of identity theft does not curtail to the need for safeguards to prevent identity theft. As the mere provision of punishment shall only be effective if the i-thief is traced, which is the major problem in the allocation of liability. With the advancement of technology, the i-thieves have become more efficient in escaping or getting traced, because their location or identity is extremely difficult to determine, as they use multiple IP addresses. Hence, the allocation of liability is a pertinent issue that needs to be resolved by the law. As suggested in the paper, the law should incorporate the concept of prevention by a person who can last avoid such occurrence, to impose liability.

Other than allocation of liability, another drawback is the lack of resources with the government to trace the offender, the government has to adopt futuristic technology in synchrony with the law to catch hold of the offender, if not, the mere law shall be an obsolete instrument.

However, in India, the lack of Data Protection laws in also a major backlash. With the increase in identity thefts, there stands a pertinent need for Data Protection laws. Therefore, the passage of the Draft Personal Data Protection Bill shall be an appreciated move towards safeguarding data and the Bill also deals with identity theft as discussed in the above chapters.

Hence, it can be concluded that an effective mechanism for curbing identity theft can be structured only upon synchrony of law and technology, because, only technology can tackle technology.

BIBLIOGRAPHY

Primary Sources:

Indian Legislations

Indian Penal Code, 1860

Information Technology Act, 2000

Foreign Legislations

Fair and Accurate Credit Transaction Act, 2003

Identity Theft and Assumption Deterrence Act, 1998

Identity Theft Enforcement and Restitution Act, 2008

Identity Theft Penalty Enhancement Act, 2004

Secondary Sources:

Books

Higgins G E, *Cyber Crime: An Introduction to an Emerging Phenomenon*, (1st edn, McGraw-Hill 2009).

Sharma B R, *Bank Frauds Prevention & Detection*, (4th edn, Universal Law Publishing Co Ltd. 2016).

Journal Articles

Anderson K B, 'Who Are the Victims of Identity Theft? The Effect of Demographics' (2006) 25 Journal of Public Policy & Marketing.

Anderson K B, Durbin E and Salinger M A, 'Identity Theft' (2008) 22 The Journal of Economic Perspectives.

Bangali S S and Bangali H S, 'In-Built Challenges for Information Technology Law in India' (2016) 4 International Journal of Advanced Research.

Brandon M, 'Financial Institutions' Duty of Confidentiality to Keep Customer's Personal Information Secure from the Threat of Identity Theft' (2001) 34 U.C. Davis Law Review.

Fawzia C , 'Protecting Personal Information In The Era Of Identity Theft: Just How Safe Is Our Personal Information From Identity Thieves?' (2015) 18 PELJ.

Fawzia C, 'Addressing the Spectre of Phishing: Are Adequate Measures in Place to Protect Victims of Phishing?' (2014) 47 The Comparative and International Law Journal of Southern Africa.

Feigelson and Calman, 'Liability for the costs of phishing and information theft' (April 2010) 13 Journal of Internet Law Technology Review.

Gillett M T, Pindexter O, McGregor V and Villongco M, 'Developments in Cyberbanking' (2004) 59 BUS LAW 1335.

Jasmine J and Rajan A, 'A Critical Study on Concept of E-Banking and Various Challenges of IT in India with Special Reference to RBI's Role in Safe Banking Practices' (2018) 119 International Journal of Pure and Applied Mathematics.

Joshi A, 'Identity Theft- A Critical and Comparative Analysis of Various Laws in India' (2009) 2 Journal on Contemporary Issues of Law.

Lele D P, Purandare S, 'Cyber Crimes as a Growing Menace' (2017) 5 International Journal of Informative and Futuristic Research.

Lynch J, 'Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks' (2005) 20 Berkeley Technology Law Journal.

Mohanty A, 'New Crimes Under the Information Technology (Amendment) Act' (2011) 7 IJLT.

Monisha H, Rajan A, 'An Analytical Study on Offences under IT Act with Special Reference to Section 66' (2018) 119 International Journal of Pure and Applied Mathematics.

*****