International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 1405-1408 www.ijaem.net ISSN: 2395-5252

Convergence of Law and Technology in Financial Sector: Legal Issues and Challenges

Shazila Shajaha, Md Jiyauddin
Research scholar , vellore institute of technology chennai
Assistant professor , northeast , frontier technical university, arunachal pradesh

Date of Submission: 12-03-2023 Date of Acceptance: 22-03-2023

ABSTRACT
People of all generations have been driven to use online modes of transactions, however with the increased usage of apps for transactions and other financial activities, the number of online banking frauds is expected to treble by 2020. Fraudsters are always looking for opportunities to profit from major world events.The resulting rapid digital acceleration fueled by stay-at-home directives, is an unprecedented global phenomenon in the digital age. Because to the pandemic's drive for contactless payments, digital fraud is on the rise due to a lack of understanding and weaknesses in personal card information. Due to local constraints and concerns about the spread of COVID, customers have been depending on digital channels to conduct business. This article examines consumer human rights in financial scams since it also deals with privacy violations, such as data theft or impersonation via virtual mode, which can result in a flagrant violation of human rights for which a remedy is difficult to get.Criminals are taking advantage of the corona virus outbreak to try to steal money by acting as banks, the government, the World Health Organization, or other health service providers, or by offering services such as a safe haven for our money or medical advice. The greater their need for immediate cash, the more vulnerable they are to loan frauds. It should be recalled that at least ten persons in Telangana committed suicide in 2020 and 2021 as a result of harassment by loan app organizers. In India, digital loan apps have been blamed for mafia-like collecting practices and suicides, with many regular people dying as a result of digital illiteracy. In order to prepare for the wave of digital transformation, it's just as necessary to acquire digital skills as it is to build digital infrastructure, starting with a steady focus on digital literacy and general literacy. Those who lack either will be marginalized and subjected to a slew of human rights violations, ranging from financial loss to identity theft. In India, digital loan apps have been blamed for mafia-like collecting practices and suicides, with many regular people dying as a result of digital illiteracy. In order to prepare for the wave of digital transformation, it's just as necessary to acquire digital skills as it is to build digital infrastructure, starting with a steady focus on digital literacy and general literacy. Those who lack either will be marginalized and subjected to a slew of human rights violations, ranging from financial loss to identity theft. A national digital literacy policy that recognizes the multifaceted nature of digital literacy and monitors the digital divide between states and localities is essential for citizens.

Keywords: Human rights, Digital frauds, Pandemic, Digital illiteracy, Technology

I. INTRODUCTION

The pandemic has caused unprecedented economic and financial instability, putting most businesses at danger of corruption, fraud, and other financial crimes. In such circumstances, it is critical to focus immediate emphasis on a strong anti-fraud and compliance structure to prevent, identify, and correct unethical behavior.Thesituation is forcing governments to make hasty decisions and take dramatic measures to safeguard vulnerable people while limiting the economic effects. Past crises have demonstrated that emergencies and the fast responses that follow generate chances for integrity violations, most notably fraud and corruption, severely limiting the effectiveness of government intervention.Many people have had to adjust to using various digital tools to manage their life as a result of the virus's threat-from working, shopping, and studying to getting entertained, paying bills, and carrying out banking operations. Banks have

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 1405-1408 www.ijaem.net ISSN: 2395-5252

had to scale up as the number of individuals utilizing internet banking has increased "Traditionally, banks have focused on three things: increasing customer revenue, lowering customer service costs, and staying current with the country's compliance and regulatory requirements.Because of the vast amount of personal and financial data they hold, the financial services industry is particularly vulnerable to cyberattacks. Emerging economies with changing regulatory and legal systems are also more vulnerable to such attacks. Cyber thieves are not always apprehended, and victims are rarely compensated, leaving them to endure the penalties and financial losses of a data breach on their own. This could be one of the reasons for the widespread concern about bank card fraud.The majority of financial frauds in India are credit card frauds, particularly incidences of card cloning, which have increased significantly in recent years. While India was one of the first countries to implement the rapid payments system, or QR code-based system, it is also one of the most secure for both banks and clients.Customers are exposed to fraudulent transactions due to a lack of sufficient end-point security at the device level. Data thieves gain KYC credentials by internet phishing via social media or e-mail, he adds, and impersonation frauds have also increased over the years. One of the reasons financial institutions have been unable to avoid such scams is the lack of a multi-layered approach to identifying frauds.Not all customer fraud occurs at the customer's end."While customer-side fraud is more visible, there has been an increase in cybercrime in the form of corporate email compromise targeting financial institution officials. The financial ecosystem is heavily intertwined, and banks must rely on alliance partners and third-party vendors in order to conduct business, rendering its security infrastructure vulnerable.

IMPACT OF TECHNOLOGY ON EMERGING BANKING CRIMES

In the twenty-first century, technology has been one of the most important developmental tools in the global corporate environment. Globalization and technology have re-defined the old metrics for evaluating market and corporate activities, resulting in increased efforts to improve efficiency in response to the creation of customer value. Although technological innovation has been seen in every business, its revolution and impact in the service sector, particularly in the banking industry, has been extremely worrying.As a result of social alienation, a rising number of people are managing their money using online banking channels. This will almost certainly lead to a more permanent change in customer preferences toward digital channels, as well as an increase in demand for digital services. Banks must be accessible to all customers, including the elderly and others who are unfamiliar with digital banking, by giving training on how to use digital tools and maintaining ATMs stocked and working.Numerous incidents like a25-year-old lady filed a case against an internet lending company for harassing, stalking, defamation, and outraging her modesty after she began receiving abusive, vulgar, and filthy texts, pictures/videos after allegedly defaulting on a Rs20,000 loan for a day. Police have filed a FIR under Indian Penal Code sections under the Information Technology Act against two online loan apps and are seeking for the perpetrators. The Delhi Police's Special Cell's Intelligence Fusion and Strategic Operations (IFSO) Unit has detained eight people from Delhi and other areas of the country for allegedly extorting money from people under the guise of providing and repaying loans.During the pandemic, digital loan apps that promised rapid cash soared in popularity across India and other developing economies. Activists claim they prey on unsuspecting borrowers, accusing them of using harsh collection tactics and charging interest rates as high as 500%, which have been linked to a number of deaths.A 36-year-old man attempted suicide after being harassed by microloan lending app businesses, authorities said. He died five days later while undergoing treatment in Visakhapatnam, Andhra Pradesh. On the evening of December 23, he died at King George Hospital. Following a complaint from his buddy, the NTPC Police Station in Rama Gundam, Telangana, has filed a case under Section 306 of the Indian Penal Code (abetment of suicide) and begun an investigation.

Shrikar Manne, a Hyderabad resident and self-employed real estate agent, failed to make an EMI loan payment on April 15 for a loan he had obtained through an instant personal loan application app. He claims that the Mumbai-based business then harassed him over the phone.They broke into his phone, accessed all of his contacts, and dialed everyone on his contact list.The firm informed their contacts that he had provided them names as a reference when he applied for the loan,Shrikar claims, that the firm made over 200 such calls to his contacts. It's against the law and unethical. They slandered him and his reputation all over the place.Shrikar had obtained a Rs 50,000 loan through Kissht, a firm that offers fast personal loans with EMI payments. Aside from fast loans, the organization also offers interest-free financing.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 1405-1408 www.ijaem.net ISSN: 2395-5252

The company is one of many such rapid loan apps available on Google Play, and it was introduced to Shikar via MakeMyTrip, a travel aggregation website.When these apps are loaded on a phone, they collect not only contact information, but they may also be able to track calls to see who is being contacted the most. Some applications have even been accused of putting tracking software inside other apps to monitor spending behavior and GPS whereabouts, with the data being used to assess a potential borrower's creditworthiness. Despite the Play Store's developer content policy, which prohibits organizations from publishing digital loan apps, some digital loan apps, particularly payday lending providers, are available on the platformthat provide only short-term personal loans which require payment in full in 60 days or less from the date the loan was issued. In response to charges that the corporation collects phone contact information from its consumers, a spokeswoman for the company stated they scrape the contacts and look for keywords, GSP, and the overall number of contacts to establish creditworthiness.

HUMAN RIGHTS VIOLATIONS ON EMERGING BANKING FRAUDS

Cybercrime has no physical borders and can damage any country on the planet. The use of information technology to modify the way people commits crimes; the law should not be a bystander but should adapt to the changing environment. In light of the changing environment, it was necessary to rewrite the existing legislation. The majority of Indian laws are determined by the physical environment, geographical barriers, palpable documents, and documents, and were either established by British government or enacted after independence during first three decades. In the digital era, everything here is recorded regardless of physical barriers. As a result of these repercussions, tough statutory rules are required to regulate illegal actions in the cyber space and to defend the technological development system.As the number of people using E-banking increases and the spectrum of online interactions expands, so does the number of cybercrimes.Internet banking is a branch of conventional banking that uses the Internet to receive consumer instructions as well as provide banking services. As a result, certain legal provisions that apply to conventional banking services can be extended to Internet banking in theory. The utilization of electronic media, particularly the Internet, in financial transactions has created concerns regarding the legality of some types of transactions under current law. The legitimacy of an electronic message or document, authentication, the legality of electronic contract, non-repudiation, and other legal issues affecting electronic commerce and Internet banking are all major legal issues. The susceptibility of data travelling across the Internet, it has also raised worries about banks' ability to comply with regulatory duties and practices such as privacy and confidentiality of clients' accounts, consumer protection, and so on. During pandemic wave of covid 19 So far, three cases of suicide have been reported in Telangana, purportedly as a result of harassment over the repayment of app-based microloans. An unemployed techie, an agriculture extension official, and a farmer are among the victims of such apps. Hundreds of cases are currently being investigated across the state in order to crack down on the operations of such digital lending platforms that operate with or without ties to Non-Banking Financial Companies (NBFCs).

LEGISLATIVE DRAWBACKS

The present legal framework does not define boundaries by which a person can be held liable for an electronic instruction that he claims to have provided. Authentication is usually accomplished through a security technique. To confirm the authenticity of an instruction, methods and techniques such as personal identification numbers (PIN), code numbers, telephone-PIN numbers, relationship numbers, passwords, account numbers, and encryption have evolved. From a legal standpoint, the security technique must be acknowledged as a substitute for signature by the law. The automation system includes several characteristics such as entire computerization of branches that are interconnected in the form of an integrated system with security controls to ensure data integrity and security. Furthermore, intangible data is stored by automationsimultaneously as mentioned in ledgers, passbooks, vouchers, statements and can be subsequently generated in tangible form.As can be seen, automation has had a positive impact on the Single Window Service System, which allows customers to approach any counter in the banking institution for any type of activity or service. The Electronic Fund Transfer (EFT) system is a result of automation that allows for the electronic transmission and processing of funds from one branch to another. Off-site Automatic Teller Machines (ATMs) linked to satellites to provide money through the use of an optical magnetic electronic processing device (debit/credit card) provide instant services to customers, and the nature of transactions is automatically entered into the relevant account in

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 1405-1408 www.ijaem.net ISSN: 2395-5252

the branch. This type of computerization capability allows clients to receive faster service while also giving banking organizations the ability to store, retrieve, and convert data for useful purposes. In basic terms, this facility automates the storing, retrieval, combing, sorting, organizing, transmitting, and processing of data to provide various services to both clients and banking organizations. Banking institutions manage deposits, withdrawals, loans, investments, foreign exchange, human resources, and all other essential information using computers.

II. CONCLUSION

Because of the country's financial reforms, the number of branches has expanded. Due to the development of the bank branch network, the internet is now used everywhere. Due to growth of banking industry, the number of customers has increased significantly, and they have become victims of cybercrime.The rise in cybercrime has a significant influence on the banking industry as a result of the expansion in bank branches in the country. Banking has shifted from conservative to technology-driven as a result of technological improvements. The frequency of cyber-crime incidences incorporating e-banking has risen significantly as ATMs have upgraded and proliferated.Customers were drawn as far as possible into the realm of e-banking, but it also presented an opportunity for cyber criminals to commitcybercrimes against e-banking. Because of the progression and expansion of ATMs, cybercrime has had a negative impact on e-banking in India.The e-banking business has grown dramatically as a result of the development of banking industry and the usage of technology. CERT-In (Indian Computer Emergency Response Team) with purpose of safeguarding Indian cyberspace.It is clear from the foregoing that India's cyber legislation and supporting regulations for e-banking operations are insufficient to combat the rising tide of cybercrime. As a result, the number of CERT-reported occurrences has increased. Based on the foregoing, we conclude that current cyber laws in India, where cybercrime is on the rise, are woefully inadequate to control cybercrimes against e-banking.Former RBI Deputy Governor Anand Sinha remarked "It is possible that total eradication of computer crimes may not be achieved. It can, however, be reduced through public education, robust law enforcement, compliance using effective security technologies and the establishment of foolproof framework for the prosecution of computer criminals," Nobody can disagree that the IT Act needs to be amended in order to make it even more efficient in mitigating cybercrime.Anand Sinha, a former deputy governor of the Reserve Bank of India, said "It's probable that computer crimes will never be completely eradicated. Public education, strong law enforcement, compliance with appropriate security technologies, and the construction of a watertight structure for prosecuting computer criminals can all help to diminish it." Nobody can deny that the Cyber laws needs to be modified in order to make it more effective in combating cybercrime.

REFERENCES

[1]. Kamath Nandan, Law relating to Computers, Internet and E-commerce: A Guide to Cyber Laws and the Information Technology Act, 2000 (Universal Law Publishing Co, 2009).

[2]. Karimzadeh M &Alam." Electronic banking challenges in India: An empirical investigation" at 45 &n.4 .Interdisciplinary Journal of Contemporary Research In Business (2012).

[3]. Khanna & Bindu Arora ," A study to investigate the reasons for bank frauds and the implementation of preventive security controls in India banking Industry," n.4. International Journal of Business Science and Applied Management, (2009).

[4]. Willson, R, "Understanding the Environment Dynamics for Computer Crimes" at.186 &n. 19. InformationTechnology Journal , (2006).